Declaración de Seguridad

KeyOne 2.1








© Copyright 1999-2006 Safelayer Secure Communications, S.A. Todos los derechos reservados.

KeyOne 2.1 Declaración de Seguridad

Este documento es propiedad intelectual de Safelayer Secure Communications, S.A. Su contenido es confidencial y el acceso está restringido a personal de Safelayer Secure Communications, S.A.

No se autoriza la copia, reproducción o almacenamiento de parte alguna de este documento de ninguna manera o por ningún medio, electrónico, mecánico, por grabación, o de ninguna otra manera, sin el permiso de Safelayer Secure Communications, S.A.

Safelayer Secure Communications, S.A.

Teléfono: +34 93 508 80 90

Fax: +34 93 508 80 91

Web: www.safelayer.com

Email: support@safelayer.com



CONTENIDO





Bibliografía, Definiciones y Acrónimos

Bibliografía

Las siguientes referencias se citan en este documento:

Reference	*Referenced document*
[CEN01a]	CEN/ISSS Workshop on Electronic Signatures. CEN *Hardware Security Modules for CSPs, CC Protection Profile*, EESSI Area D2, 2001.
[CEN01b]	CEN/ISSS Workshop on Electronic Signatures. *CEN/ISSS WS/E-Sign Workshop Agreement Group F, Security Requirements of Secure Signature Creation Devices (SSCD)*, 2001.
[CEN01c]	CEN/ISSS Workshop on Electronic Signatures. *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures*, June 2003.
[CEN CMCSO-PP]	CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 4: Cryptographic module for CSP signing operations – Protection profile – CMCSO PP
[Eur99a]	European Community. *Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the "Electronic Signature Committee" in the Directive.*, 1999.
[Eur99b]	European Community. *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures*, 1999.
[FIP]	*FIPS 140-1 SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES.*
[Ser97]	Service Central de la Sécurité des Systèmes d'Information. *Expression des Besoins et Identification des Objectifs de Sécurité*, 1.02 edition, 1997.



Reference	*Referenced document*
[the99a]	the Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation* Part 3: Security assurance requirements, 2.2, January 2004.
[the99b]	the Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation*, 2.2. January 2004.
[the99c]	the Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model*, 2.2, January 2004.
[TS1]	ETSI TS 101 456, *Policy Requirements for Certification Authorities Issuing Qualified Certificates*.
[FUNCSPEC]	KeyOne 2.1 – Product Specification, Safelayer internal code: 4C988209
[K121STRENGTHFUNC]	KeyOne 2.1 – Strength of Functions Analysis, Safelayer internal code: CD1646E8
[ALGO]	ETSI SR 002 176 – Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures
[X509]	X509v3: ITU-T Recommendation X.509 | ISO/IEC International Standard 9594-8, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
[TS101862]	ETSI TS 1O1 862, Qualified Certificate Profile
[PKCS5]	PKCS #5: Password-Based Encryption Standard, RSA Laboratories
[RFC2560]	RFC 2560: Online Certificate Status Protocol - OCSP
[RFC3161]	RFC 3161: Time-Stamp Protocol (TSP)
[Eur03c]	*COMMISSION DECISION of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council*
[CONFGUIDE]	Configuration Guide – CC EAL2 Certification -, Safelayer internal code: 0F92B8A5



Definiciones

Datos de Activación: Datos distintos a las claves, que son necesarios para la operación con módulos criptográficos y que deben ser protegidos (ej.: un PIN, una frase de paso o una llave física compartida)

Firma electrónica avanzada: es la firma electrónica que cumple los requisitos siguientes:

- Estar vinculada al firmante de manera única,
- Permitir la identificación del firmante;
- Haber sido creada utilizando medios que el firmante pueda mantener bajo su exclusivo control
- Estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable.

CA-certificado: Un certificado para una CA, emitido por otra CA.

Punto de Distribución de CRL: Una entrada de directorio u otra fuente de distribución para CRLs; una CRL que se distribuye mediante un punto de distribución de CRL, sólo puede contener un subconjunto del conjunto de certificados emitidos por una CA y puede contener entradas de revocación de múltiples CAs.

Servicio de Publicación de Certificados: Un servicio de difusión de los certificados para los subscriptores y para otras Partes de Confianza, siempre que exista consentimiento del subscriptor. Este servicio también publica la información de política y prácticas a los Subscriptores y Partes de Confianza

Servicio de Generación de Certificados: Un servicio que genera y firma certificados basados en la identidad y demás atributos que sean verificados por el servicio de registro.

Política de Certificación: Un conjunto de reglas a saber que indican la aplicabilidad de un certificado dentro de una comunidad particular y/o una clase de aplicación con requisitos de seguridad comunes.

Periodo de validez del certificado: El periodo de validez del certificado es el intervalo de tiempo durante el cuál la CA garantiza el mantenimiento del estado del certificado.

Certificado: La certificación electrónica que vincula unos datos de verificación de firma a una persona, y confirma la identidad de ésta.

Declaración de Prácticas de Certificación: Una declaración de las Prácticas que emplea una Autoridad de Certificación para emitir certificados.

Autoridad de Certificación (CA): Una Autoridad de confianza para uno o más usuarios, que genera y asigna certificados. De forma opcional, la Autoridad de Certificación puede generar las claves de usuario

Camino de Certificación: Una cadena de varios certificados, entre los que se encuentra un certificado de la clave pública del propietario (entidad final) firmado por la CA, y cero o más certificados de Cas adicionales firmados por otras Cas.



Proveedor de Servicios de Certificación: una entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica;

Firma Digital: Datos anexos, o transformados mediante criptografía (ver criptografía), de una unidad de datos que permite a un receptor probar su procedencia y la integridad de dicha unidad de datos y protegida contra falsificaciones, por ej. del receptor.

Firma Electrónica: Datos en formato electrónico, anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación

Producto de firma electrónica: Hardware, software u otros componentes específicos que se destinan a ser utilizados por el proveedor de servicios de certificación para la prestación de servicios de firma electrónica o que se destinan a ser utilizados para la creación o la verificación de firmas electrónicas.

Entidad Final: Un sujeto del certificado que utiliza su clave pública para propósitos distintos a la firma de certificados.

Función Hash: Una función que asocia una cadena de bits a una cadena de longitud fija, que cumple las dos propiedades siguientes:

- Es computacionalmente imposible a partir de un determinado resultado encontrar el dato de entrada correspondiente.
- Es computacionalmente imposible a partir de una entrada encontrar una segunda que genere idéntico resultado.

Calificador de Política: Información dependiente de política que acompaña al identificador de política en un certificado X.509.

Clave Privada: La clave de un par de claves asimétricas de una entidad, que sólo debería ser usada por dicha entidad.

Clave Pública: La clave de un par de claves asimétricas de una entidad que puede hacerse pública.

Certificado Reconocido: un certificado que cumple los requisitos establecidos en el anexo I de la Directiva y es suministrado por un proveedor de servicios de certificación que cumple los requisitos establecidos en el Anexo II de la Directiva.

Firma electrónica reconocida: Una firma electrónica avanzada, basada en un certificado reconocido y que ha sido creada con dispositivos de creación de firma seguros (Nota: Definición de firma extractada de la Directiva)

Servicio de Registro: Un servicio que verifica la identidad y demás atributos del subscriptor, cuando sea de aplicación. Los resultados de este servicio se pasan al Servicio de Generación de Certificados.

Autoridad de Registro (RA): An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). La entidad responsable de la identificación y autenticación de los sujetos del certificado, pero no responde de la firma y emisión de los certificados (es decir, la CA delega ciertas tareas en la LRA)

Parte de Confianza: Un usuario o agente que confía en los datos de un certificado para la toma de decisiones.

Servicio de Gestión de Revocación: un servicio que proporciona los procesos de informe y petición relativos a la revocación que determinan la acción a tomar. Los resultados de este servicio se difunden a través del servicio de estado de revocación.

Servicio de Estado de Revocación: Un servicio que proporciona información del estado de revocación de un certificado a las partes de confianza. Este servicio puede ofrecerse en tiempo real o basarse en la información sobre el estado de revocación, que se actualiza a intervalos regulares.

Dispositivo seguro de creación de firma: un dispositivo de creación de firma que cumple los requisitos establecidos en el Anexo III de la directiva.

Política de Seguridad: Conjunto de reglas establecidas por una Autoridad de Seguridad que regula el uso y la provisión de servicios y facilidades de seguridad.

Certificado Auto-firmado: Un certificado de CA firmado por la propia CA

Firmante: La persona que está en posesión de los datos de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa.

Datos de Creación de firma: son los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear una firma electrónica.

Dispositivo de Creación de Firma: Es el software o hardware utilizado para aplicar los datos de creación de firma

Dispositivo de Verificación de Firma: Es el software o hardware utilizado para aplicar los datos de verificación de firma

Datos de Verificación de firma: son los datos tales como códigos o claves criptográficas públicas, que se utilizan para la verificación de una firma electrónica.

Servicio de Suministro de Dispositivo de Usuario: Es el servicio que prepara y proporciona el Dispositivo de Creación de Firma a los subscriptores.

Subscriptor: Una entidad que suscribe un contrato con el CSP para obtener su clave pública y la certificación de su identidad mediante un certificado de clave pública.

Servicio de Sellado de Tiempo: Este servicio proporciona un vínculo entre unos datos y un instante de tiempo, para establecer evidencias fiables de que un dato existió en un momento determinado.

Sistema Fiable: Un sistema de información o producto implementado en hardware y/o software que genera registros auténticos y fiables, que están protegidos frente modificaciones, garantizando además, la seguridad técnica y criptográfica de los procesos que se apoyan en el mismo.

Acreditación voluntaria: Todo permiso que establezca derechos y obligaciones específicas para la prestación de servicios de certificación, que se concedería a petición del proveedor de servicios de certificación interesado, por el organismo público o privado, encargado del establecimiento y supervisión del cumplimiento de dichos derechos y obligaciones, cuando el proveedor de servicios de certificación no esté habilitado para ejercer los derechos derivados del permiso hasta que haya recaído la decisión positiva de dicho organismo.



Acrónimos

Los siguientes acrónimos se utilizan a lo largo del documento:

Acrónimo	*Significado*
ARL	Lista de Revocación de Autoridades
CA	Autoridad de Certificación
CP	Política de Certificación
CRL	Lista de Revocación de Certificados
CSP	Proveedor de Servicios de Certificación
HSM	Módulo de Seguridad Hardware
HW	Hardware
I/O	Input/Output
It	Tecnología de la Información
NQC	Certificado no reconocido
OCSP	Protocolo online del estado de certificado
OS	Sistema Operativo
PKI	Infraestructura de Clave pública
POP	Prueba de Posesión
PP	Perfil de Protección
QC	Certificado Reconocido
RA	Autoridad de Registro
SCD	Dispositivo de Creación de Firma
SF	Función de Seguridad
SSCD	Dispositivo de Creación de Firma Seguro
ST	Declaración de Seguridad
TOE	Objeto de Evaluación
TSA	Autoridad de Sellado de Tiempo
TSS	Servicio de Sellado de Tiempo
KTS	Sistema Fiable KeyOne

CAPÍTULO 1

Introducción

Identificación

ID Documento: 040A5EBD v2.1

Título Declaración de Seguridad KeyOne 2.1

ID Distribución 04S1R2

Autores Safelayer Secure Communications S.A..

Estado Publicado

Versión CC: 2.2 Final

TOE evaluado: KeyOne 2.1.04S1R2: KeyOne CA, KeyOne LRA, KeyOne VA, KeyOne TSA

Parches: 2.1.04S1R2_B25

Visión General

El propósito de esta Declaración de Seguridad es especificar los requisitos de seguridad funcionales y de garantía implementados por KeyOne 2.1 TWS, que es el Objeto de Evaluación.

El contenido de este documento está estructurado en los siguientes capítulos:

Capítulo 1, proporciona la información descriptiva y el etiquetado de la Declaración de Seguridad y del Objeto de Evaluación al que hace referencia, un resumen del Objeto de Evaluación y una declaración de conformidad con requisitos CC.

Capítulo 2, proporciona una descripción de los servicios que proporciona el Objeto de Evaluación, da una visión general de los usuarios que interaccionarán con el Objeto de Evaluación, y describe las arquitecturas lógicas y físicas del sistema, así como la contribución de cada subsistema a los servicios identificados. Finalmente, se proporciona una lista con los principales servicios de seguridad cubiertos por el Objeto de Evaluación y la utilidad de las mismas en aplicaciones de negocio potenciales.



Capítulo 3, se define el problema de seguridad, mostrando los supuestos de uso seguro que deben mantenerse, los activos que deben protegerse, las amenazas que deben contrarrestarse, y las políticas de seguridad organizativas que se deben cumplir, por el Objeto de Evaluación y su entorno operativo.

Capítulo 4, contiene la solución al problema de seguridad planteado, proporcionando los objetivos de seguridad para el Objeto de Evaluación y para el entorno.

Capítulo 5, proporciona un conjunto de requerimientos funcionales y de garantía, siguiendo el formato de requisitos de la parte 2 del CC, requisitos funcionales extendidos, requisitos de la parte 3 del CC y requisitos de garantía extendidos, para cubrir los objetivos de seguridad.

Capítulo 6, proporciona una explicación de cómo estos requisitos de seguridad son implementados en el Objeto de Evaluación.

Capítulo 7, contiene reclamaciones de conformidad ni con Perfiles de Protección ni con un estándar internacional.

Capítulo 8, proporciona la justificación de los objetivos de seguridad, mediante la resolución del problema de seguridad siempre que todos los objetivos se alcancen, y la justificación de los requisitos de seguridad, demostrando la efectiva trazabilidad entre requisitos y objetivos de seguridad. Se incluyen dos secciones más para justificar las dependencias no satisfechas y para definir los nuevos componentes extendidos.

Apéndice A pretende proveer una línea directiva para la producción de Políticas de Certificación y Declaraciones de Prácticas de Certificación para establecer un Servicio de Provisión de Certificados con el soporte del sistema KeyOne 2.1 y compatible con la Declaración de Seguridad. Este gestiona a alto nivel los temas más importantes, y los requisitos mínimos a tener en cuenta para que se corresponda con la configuración evaluada, cuando el sistema se pone en marcha y se utiliza.

Para una mejor claridad y comprensión de esta Declaración de Seguridad, se hace una explicación del marco legal aplicable a infraestructuras de certificación digital.

La Directiva Europea [Eur99b] establece un marco de requisitos para el uso de las firmas electrónicas con reconocimiento legal equivalente a las firmas manuscritas. Introduce el concepto de “firmas electrónicas avanzadas”, aquéllas que pueden ser verificadas usando Certificados Cualificados.

El Anexo II de [Eur99b] proporciona los requisitos que ha de cumplir un Proveedor de Servicios de Certificación (CSP) que emite Certificados Cualificados (QCs). Esta Declaración de Seguridad se supone que proporciona algunos de los requisitos de seguridad técnicos para el Sistema Fiable KeyOne (TWS-KeyOne), de acuerdo con [CEN01c]. Concretamente, de acuerdo con algunos de los puntos del Anexo II de [Eur99b], los Proveedores de Servicios de Certificación deben:

“(f) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan;

“(g) tomar medidas contra la falsificación de certificados y, en caso de que el proveedor de servicios de certificación genere datos de creación de firma, garantizar la confidencialidad durante el proceso de generación de dichos datos”

Para la definición de los requerimientos de seguridad recogidos en este documento, se ha considerado [CEN01c] como una referencia normativa. Esto también quiere decir que un Proveedor de Servicios de Certificación que utilice el sistema fiable de KeyOne conforme a esta Declaración de Seguridad, requerirá una configuración mínima para cumplir los requerimientos de política del sistema, que refleja [TS1].

El Objeto de Evaluación definido en esta declaración de seguridad proporciona los siguientes servicios propios de Proveedores de Servicios de Certificación:

- Registro de la información del subscriptor
- Generación de Certificados
- Gestión de Revocación de Certificados
- Servicio de Consulta del Estado de Revocación del Certificado
- Servicio de Sellado de Tiempo
- Servicio de fabricación de dispositivos de creación de firma segura (Servicio de Suministro de dispositivos de usuario)

Conformidad

En esta Declaración de Seguridad, no se hace declaración expresa de conformidad con ningún Perfil de Protección certificado. Sin embargo, sí se han tenido en cuenta los requisitos de seguridad aplicables a Proveedores de Servicios de Certificación que emiten certificados de firma electrónica, cumpliendo con las recomendaciones de la Comisión Europea, tal y como se presenta en [Eur03c]. Para la especificación de los requisitos de seguridad se han utilizado las siguientes referencias:

a. Requisitos Funcionales de Seguridad de la Parte 2 del CC.

b. Requisitos Funcionales de Seguridad Extendidos, expresados en formato CC.

c. Requisitos de Garantía de Seguridad de la Parte 3 del CC, obtenidos del paquete EAL2.

d. Requisitos de Garantía de Seguridad Extendidos, expresados en formato CC.

CAPÍTULO 2

Descripción del TOE

Aunque [Eur99b]tiene un enfoque muy general y habla sobre las firmas electrónicas de cualquier tipo, en este documento se parte de la base de que las firmas electrónicas se generan mediante criptografía de clave pública, que el subscriptor utiliza un par de claves criptográficas, una privada y otra pública, y que el certificado emitido por un sistema de confianza asocia la clave pública del subscriptor a la identidad u otra posible información del mismo, mediante una firma electrónica generada con la clave privada (clave de firma de certificado) del Objeto de Evaluación. Están fuera del ámbito de este documento, cualquier otra forma de firma electrónica.

Aunque los requisitos de seguridad para el servicio opcional de Suministro de Dispositivo de Usuario, que proporciona el Dispositivo Seguro de Creación de Firma a los usuarios subscriptores, quedan incluido en el ámbito de esta Declaración de Seguridad, los requerimientos propios de estos dispositivos, como su uso por los subscriptores están fuera del ámbito de este documento. Los requerimientos de seguridad para Dispositivos de Creación de Firma Segura se encuentran en documento aparte [CEN01b].

Siguiendo los principios de [Eur99b] esta Declaración de Seguridad pretende ser lo más independiente de la tecnología, que sea posible. No requiere, ni define ningún protocolo de comunicación en particular o formato para las firmas electrónicas, certificados, listas de revocación, información del estado del certificado y sellos de tiempo. De acuerdo con el Anexo I de la Directiva Europea, sólo se supone que los certificados han de contener determinado tipo de información. La interoperabilidad entre los sistemas del Objeto de Evaluación y los sistemas del subscriptor está fuera del ámbito de este documento.

El uso de Sistemas fiables KeyOne conformes a los requerimientos de Certificados Cualificados, indica que la tecnología usada por el Objeto de Evaluación es capaz de cumplir con los requerimientos de los Anexos I y II de la Directiva.

Más detalles de cómo se alcanza este cumplimiento se pueden encontrar en la sección 6. Mediante el uso de Sistemas Fiables KeyOne conformes con esta Declaración de Seguridad, los Objetos de Evaluación pueden llegar a reducir su carga de auditoría, auditando sólo los aspectos de operación de los sistemas y no los componentes ya evaluados.



Directiva Europea

Los requisitos del Anexo II (f) y (g) son el principal foco de esta Declaración de Seguridad, aunque es importante además abarcar los siguientes requisitos de [Eur99b]:

1 Anexo II a) demostrar la fiabilidad necesaria para prestar servicios de certificación;

2 Anexo II b) - garantizar la utilización de un servicio rápido y seguro de guía de usuarios y de un servicio de revocación seguro e inmediato;

3 Anexo II c) - garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado;

4 Anexo II i) - registrar toda la información pertinente relativa a un certificado reconocido durante un período de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos;

5 Anexo II j) - no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de gestión de claves;

6 Anexo II l) utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que:

- sólo personas autorizadas puedan hacer anotaciones y modificaciones,
- pueda comprobarse la autenticidad de la información,
- los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado, y
- el agente pueda detectar todos los cambios técnicos que pongan en entredicho los requisitos de seguridad mencionados

7 Anexo I – Requisitos de los certificados reconocidos.

Descripción del Sistema Fiable KeyOne 2.1

El KTS, en esta especificación, emite y gestiona certificados para soportar la firma electrónica. La hipótesis principal es que el Objeto de Evaluación utilizará una Infraestructura de Clave Pública (PKI) para la gestión de certificados. Esta especificación está orientada hacia el conjunto de servicios que ofrece el Objeto de Evaluación, cada uno de ellos tiene definidas unas funciones que facilitan la entrega del servicio. A su vez, cada función tiene que cumplir un mínimo de estándares de seguridad, para alcanzar el estado de confianza necesario.

El Objeto de Evaluación consiste en un conjunto de subsistemas, que proporcionan una funcionalidad específica al mismo. Aunque esta especificación considera los requisitos de seguridad de los subsistemas que participan en los servicios del Objeto de Evaluación, el objetivo es proporcionar a los subscriptores y partes de confianza

una visión sencilla del Objeto de Evaluación y, por lo tanto, también de los subsistemas que emplea para ello. Para garantizar esto, la interfaz del cliente, en esta especificación, es el “Servicio del Objeto de Evaluación” y no directamente, los servicios individuales que ofrece el Objeto de Evaluación. Los subsistemas son a su vez descompuestos, en otras funcionalidades que se referencian y vienen definidas por otros estándares aceptados.

El Objeto de Evaluación proporciona servicios mediante el despliegue de subsistemas con Funcionalidad Básica y otros servicios opcionales mediante el despliegue de subsistemas con Funcionalidad Adicional. El Objeto de Evaluación implementa dicha Funcionalidad Básica para cumplir con los requisitos de [CEN01c]. El Objeto de Evaluación, implementa también servicios opcionales, además de los servicios obligatorios, tal y como se definen en [CEN01c], junto con los requisitos de seguridad que se establecen para cada servicio en [CEN01c].

En consecuencia, el Objeto de Evaluación distribuye subsistemas que cumplen con los requisitos de Seguridad Generales y Básicos. Es importante destacar que esta integración técnica y de seguridad, no impide que los diferentes componentes del servicio del Objeto de Evaluación puedan ser libremente utilizados por distintas entidades de negocio.

Servicios Básicos del Objeto de Evaluación

Los servicios básicos que proporciona el Objeto de Evaluación son:

Servicio de Registro: Verifica la identidad y atributos específicos del subscriptor, cuando existan. Los resultados de este servicio se pasan al Servicio de Generación de Certificados.

- Solicitud de Certificación

  La solicitud de certificación la realiza el Servicio de Registro una vez que el subscriptor ha sido identificado, de acuerdo a los requisitos especificados en la política de Certificación correspondiente (ej. [TS1]).

- Gestión de los datos del subscriptor

  Dada la naturaleza del Servicio de Registro, éste debe gestionar los datos de subscriptores o entidades finales. Estos datos pueden estar afectos por diversos requisitos de protección de datos personales.

Servicio de Generación de Certificados: Crea y firma certificados basados en la identidad o algún otro atributo del subscriptor, verificados en el Servicio de Registro.

- Generación de Certificado

  Una vez recibida la petición de certificación procedente del Servicio de Registro, el sistema fiable KeyOne genera un certificado con la clave pública suministrada. Esto garantiza que el Proveedor de Servicios de Certificación ha bloqueado la asociación de la clave pública del subscriptor con su identidad.



Los sistemas fiables KeyOne también pueden enviar las claves de infraestructura[1] y de control[2] a este servicio para que sean certificadas por él. Esto proporciona los certificados de Control y de Infraestructura.

Continuando con la generación del certificado, el certificado es directamente entregado al subscriptor, y además puede ser distribuido por el Servicio de Divulgación de Certificados (publicación del certificado en un directorio).

Los certificados de Control e Infraestructura se pueden proporcionar directamente al componente de confianza que lo requiera.

- Renovación del certificado

  Durante el periodo anterior a la expiración del certificado, que viene definido en la política, el certificado puede ser renovado. La renovación del certificado consiste en la renovación de la clave, de acuerdo al siguiente escenario: se certifica una nueva clave usando la información de registro que se utilizó para generar el certificado anterior. La renovación de certificados contempla los certificado de subscriptor, de control y de infraestructura.

Servicio de Gestión de revocación: Los procesos de informe y petición relativos a la revocación que determinan la acción a tomar. Los resultados de este servicio se difunden a través del servicio de estado de revocación.

- Peticiones de cambio de estado del certificado

  Cuando un subscriptor sospechara que su clave privada puede estar comprometida, se envía una petición de suspensión (revocación temporal) de certificado en cuestión al KTS del Proveedor de Servicios de Certificación que lo emitió. La petición correspondiente de reactivación de un certificado suspendido debe hacerla el propio subscriptor.

  Cuando el subscriptor sabe realmente que la clave privada ha sido comprometida, se envía una petición de revocación del certificado al KTS del Proveedor de Servicios de Certificación que lo emitió.

  El Proveedor de Servicios de Certificación puede también solicitar un cambio de estado de su certificado, a través de este servicio.

- Revocación / Suspensión del certificado

  Una vez obtenida la petición de suspensión o revocación por el KTS, se cambia el estado del certificado a suspendido o a revocado (figura 2.1: mensaje A) dentro de la base de datos de estado de los certificados, que será, a su vez usado por el Servicio de estado de revocación.

Servicio de Estado de Revocación: Proporciona información del estado de revocación de un certificado a las partes de confianza. Este servicio se basa en la información sobre el estado de revocación, que se actualiza a intervalos regulares.

---

[1] *Las claves de Infraestructura son utilizadas por los propios componentes del Objeto de Evaluación para los procesos de autenticación de subsistemas, firmado de registros de auditoría, transmisión de datos cifrados,....*

[2] *Las claves de control son utilizadas por el personal que gestiona u opera con los componentes del Objeto de Evaluación, proporcionando servicios de confidencialidad, firma o autenticación al personal que interactúa con el sistema.*

- Datos sobre el estado de revocación

  Proporciona información del estado de revocación de un certificado a las partes de confianza. Este servicio refleja los cambios en el estado del certificado, provocados por peticiones de cambio de estado procedentes del subscriptor o por el CSP, que son procesadas por el Servicio de gestión de Revocación. Estos datos pueden estar también disponibles para el subscriptor, si la política así lo requiere.

- Petición/Respuesta del estado

  Una Parte de Confianza que accede a un certificado mediante el Servicio de Directorio, para verificar una firma, requiere chequear el estado de estos certificados. El CSP proporciona un Servicio de Consulta del Estado de Revocación con este propósito. En la arquitectura del sistema KeyOne, el servicio de estado de revocación es un servicio "online", que utiliza mensajes periódicos entre el Servicio de Estado de Revocación y el Servicio de Gestión de Revocación.

  En este servicio "online", la Parte de Confianza se comunica con el Servicio de Estado de Revocación, proporcionándole detalles de los certificados para los que se solicita el estado. Este servicio online, que utiliza mensajes periódicos, hace las consultas a sus registros internos, que habrán sido actualizados con el último mensaje. Así, se genera una respuesta y se envía a la Parte de Confianza indicando el estado del certificado solicitado.

  La Figura 2.1 muestra la relación entre el Servicio de Gestión de revocación y el Servicio de Estado de Revocación. En la figura, el mensaje A actualiza la base de datos de estado de los certificados, mientras que el mensaje B, es una petición /respuesta.



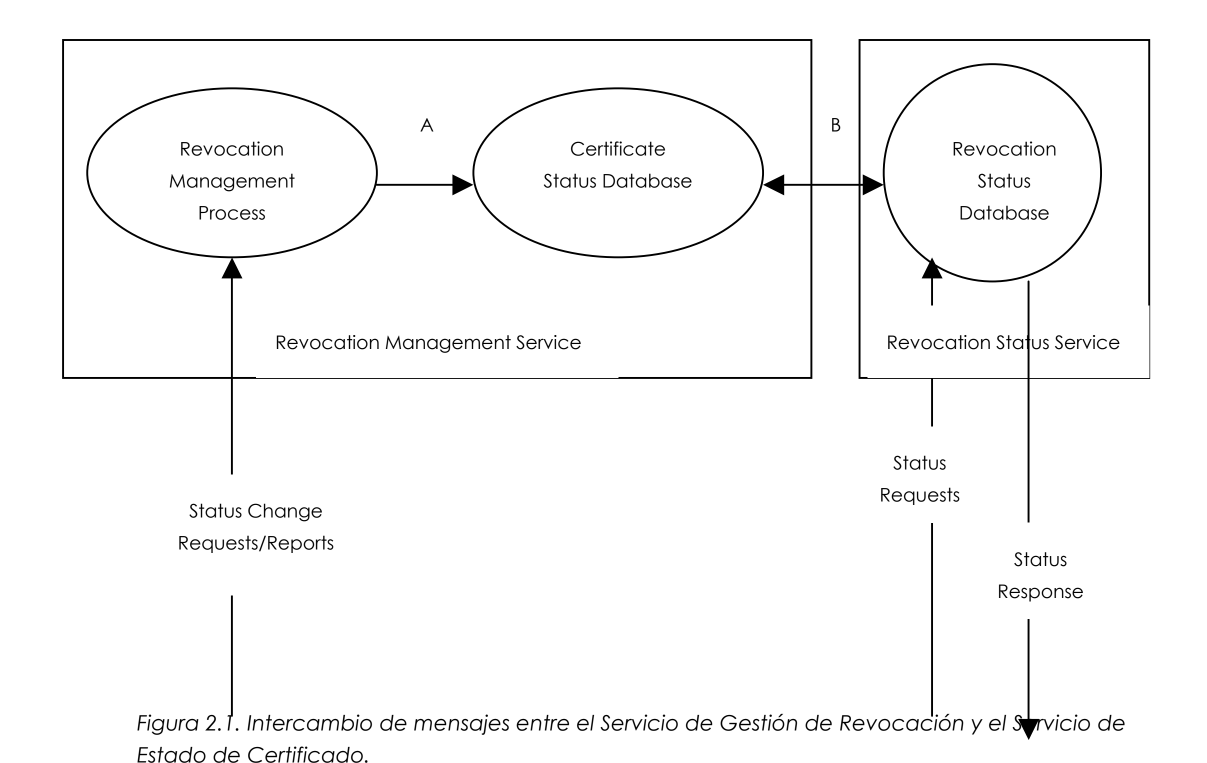


Figura 2.1. Intercambio de mensajes entre el Servicio de Gestión de Revocación y el Servicio de Estado de Certificado.

Servicios Adicionales del Objeto de Evaluación

El Sistema Fiable KeyOne también proporciona los siguientes servicios adicionales, identificados como opcionales en [CEN01c]:

Servicio de Suministro de Dispositivo de Usuario: Prepara y proporciona a los subscriptores el Dispositivo de Creación de Firma.

Es importante destacar que este servicio puede proporcionar tanto un SCD, como un SSCD. En el ámbito de esta declaración de seguridad, los requisitos de seguridad aplicables a SCDs, son igualmente aplicables a SSCDs, cumpliendo además los requerimientos que se establecen en el Anexo III de la [Eur99b]. No se hace distinción alguna de si el SCD/ SSCD es implementado en software o en hardware.

- Preparación del SCD

  El Sistema Fiable KeyOne del Proveedor de Servicios de Certificación prepara el dispositivo mediante la creación de la estructura de fichero, formateado e inicialización necesarias.

  El Sistema Fiable KeyOne ordena al SCD, la generación del par de claves dentro del mismo.

- Suministro del SCD

  El suministro del SCD es la distribución del mismo al subscriptor (una vez preparado).

- Distribución y creación de los datos de Activación



El SCD está protegido mediante unos datos de activación (secretos), que protegen el contenido del SCD. El Proveedor de Servicios de Certificación es responsable de la generación de los datos de activación y su posterior distribución al subscriptor.

Servicio de Sellado de Tiempo: Una tercera Parte de confianza, proporciona el servicio de sellado de tiempo. Este servicio proporciona pruebas de la existencia de unos datos en un instante de tiempo determinado (prueba de existencia). Si los datos fueron firmados por el peticionario, antes de ser enviados a la Autoridad de Sellado de Tiempo (TSA), entonces este servicio proporciona una prueba, de la existencia de los datos y de que fueron firmados en ese instante de tiempo.

- Revisión de la corrección de la petición

  Este componente está diseñado para revisar que la petición es completa y correcta. Si el resultado es positivo, los datos se envían como entrada a la Generación de Sello de Tiempo.

- Generación del parámetro tiempo

  Este componente usa una fuente de confianza para la distribución de parámetros de tiempo. Estos parámetros serán usados como entrada al proceso de Generación de Sellado de Tiempo.

- Generación de Sello de Tiempo

  Esta función es la responsable de crear un sello de tiempo que asocie el instante de tiempo actual, un número de serie único, los datos proporcionados para el sellado de tiempo y garantizar los requerimientos de política a la que se adhiere.

- Time Stamp Token (TST)

  Este componente calcula el indicador del sello de tiempo que se devolverá al cliente. Es el que realmente hace la firma criptográfica de los datos que proporciona la función de generación del indicador de sello de tiempo.

La figura 2.2 muestra una TSA conceptual proveyendo el servicio de sellado de tiempo.

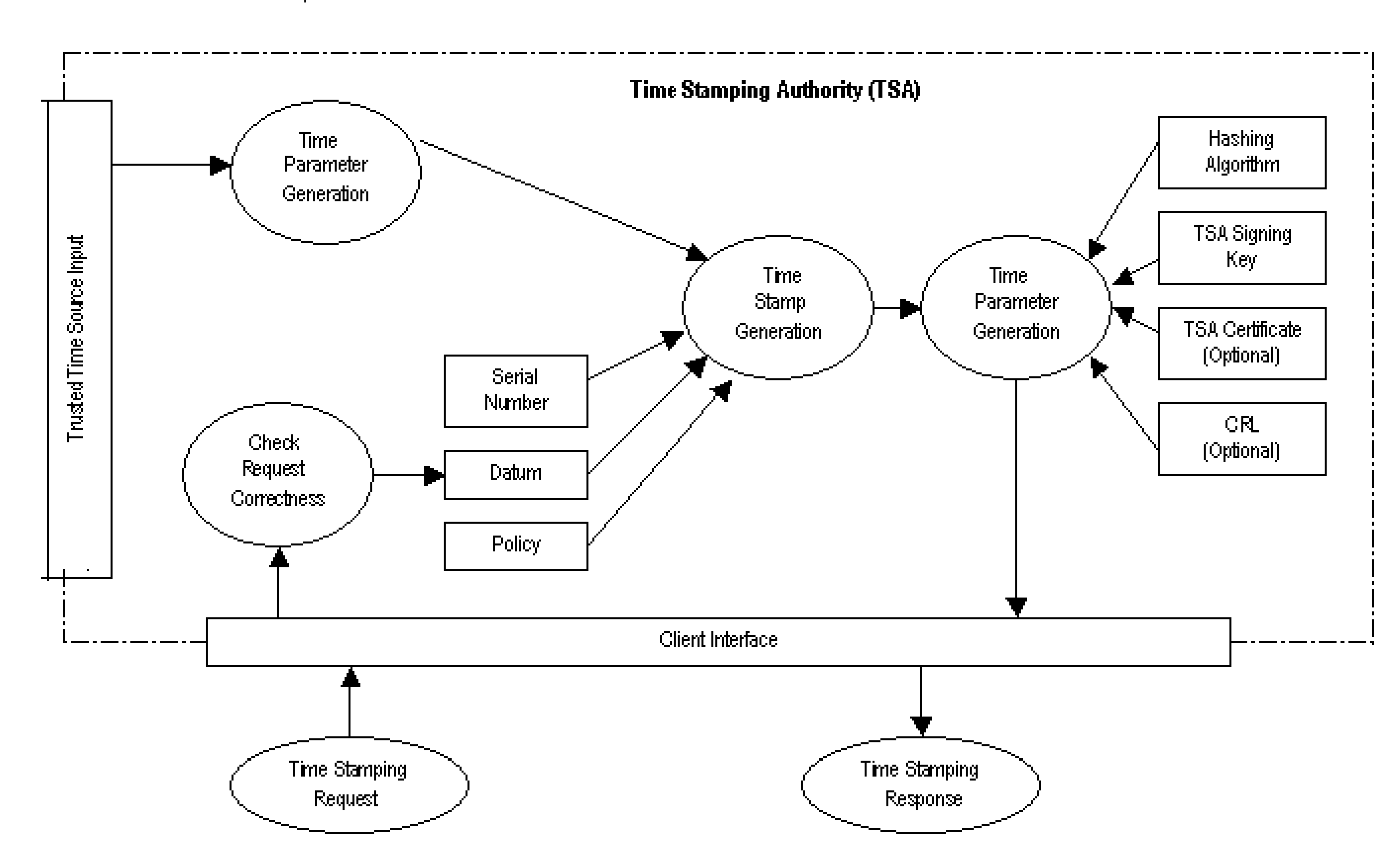




Figura 2.2. Servicios de Sellado de Tiempo

Usuarios del Objeto de Evaluación

Los usuarios a los que se dirigen los servicios del Objeto de Evaluación se clasifican en dos grupos principales:

Usuarios Externos

El usuario final / Entidad Certificada es el sujeto del certificado al que se asocia su identidad con su clave pública. Hay otros tipos de entidades que pueden certificarse, como por ejemplo aplicaciones, servidores.

Las Partes de Confianza, usuarios o agentes o cualquier servicio de confianza externo, que confíe en los datos de un certificado a la hora de tomar decisiones, siguiendo los procesos de verificación y limitaciones que se establecen en las políticas de certificación para cada tipo de certificado emitido por el sistema fiable KeyOne.

Entidades auditoras, que necesitan acceder a las trazas de auditoría para llevar a cabo los procesos de evaluación para revisar el cumplimiento de las prácticas de certificación.

Usuarios Internos

Administradores de la PKI, que pueden configurar y administrar las distintas aplicaciones de la TOE: Registro, Autoridad de Certificación, Autoridad de Validación, Autoridad de Sellado de Tiempo.

El Oficial de Registro es responsable de la operación de la Autoridad de Registro Local, de acuerdo a los procedimientos de registro establecidos.

Visión General de la Arquitectura

La arquitectura lógica del Objeto de Evaluación se muestra en la figura 2.3, donde puede apreciarse fácilmente la generación y el uso de una transacción firmada, desde que es iniciada por el subscriptor hasta que llega a la parte que confía. Esta figura ilustra tanto los servicios obligatorios como los opcionales, los interfaces del Objeto de Evaluación con los subscriptores, las partes de confianza y con cualquier otro Servicio Fiable.

Figura 2.3. Visión General de la arquitectura

Como muestra la figura, el Objeto de Evaluación proporciona tanto el registro inicial como la generación de certificados. Principalmente, la gestión del ciclo de vida del certificado (cuando no existen estados de revocación o suspendido) se proporcionan mediante el Registro y la Generación de Certificados. De forma secundaria, siempre que existan estados del certificado excepcionales, la gestión del ciclo de vida del certificado será proporcionado por los servicios de Gestión de Revocación y de Consulta del Estado del Certificado.

La interfaz de cliente del Objeto de Evaluación proporciona acceso a los servicios del Objeto de Evaluación tanto a los subscriptores como a las partes de confianza. La interfaz para los Servicios Confiables Externos, proporciona acceso a los servicios externos de otros Objetos de Evaluación, servicios de archivos confiables, etc.. Un objeto de evaluación puede utilizar varios sistemas fiables KeyOne para proporcionar tanto los servicios básicos, como los adicionales, cuando sea necesario.

Arquitectura Lógica

La arquitectura lógica del sistema fiable KeyOne se muestra en la siguiente figura:



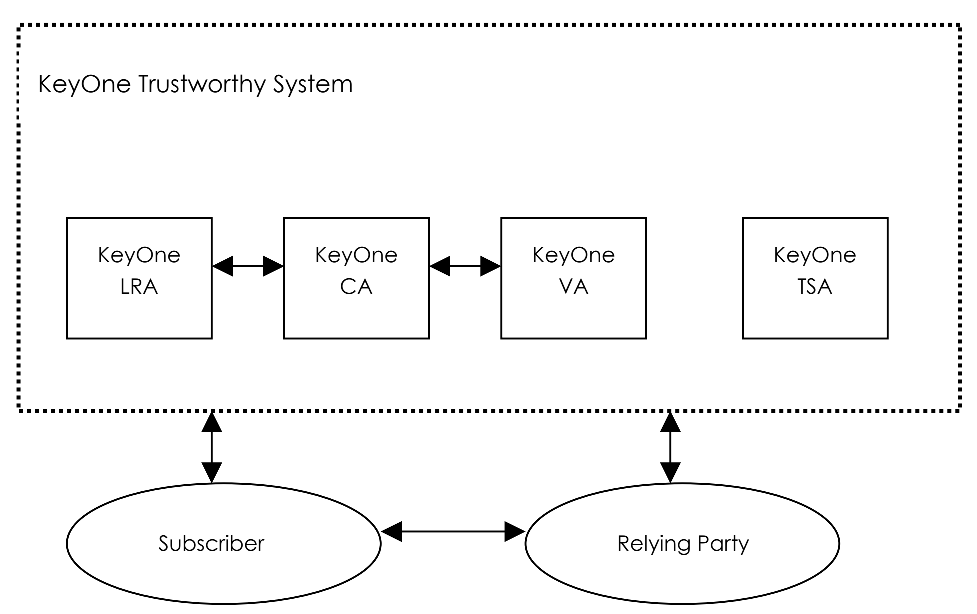


Figura 2.4. Arquitectura Lógica del KTS

Por tanto, el sistema KeyOne consta de los siguientes elementos:

- KeyOne LRA. Los servicios relativos a este componente KeyOne se explican en la sección de Servicios Básicos del Objeto de Evaluación, página 13.
- KeyOne CA. Los servicios relativos a este componente KeyOne se explican en la sección de Servicios Básicos del Objeto de Evaluación, página 13.
- KeyOne VA. Los servicios relativos a este componente KeyOne se explican en la sección de Servicios Adicionales del Objeto de Evaluación, página 16.
- KeyOne TSA. Los servicios relativos a este componente KeyOne se explican en la sección de Servicios Adicionales del Objeto de Evaluación, página 16.

Servicios Soportados

Esta tabla enumera los servicios soportados por el sistema:

Subsistema	Servicios
KeyOne LRA	Servicio de Registro Servicio de Suministro de Dispositivos de Usuario
KeyOne CA	Servicio de generación de Certificados Servicio de Gestión de Revocación
KeyOne VA	Servicio de Estado de Revocación
KeyOne TSA	Servicio de Sellado de tiempo

Tabla 2.1. Servicios soportados por el sistema

Servicios de Gestión de Revocación, Generación de Certificados y Registro

El subscriptor del servicio de certificación hace una petición de certificación a la KeyOne LRA, que una vez verificada la identidad del subscriptor, redirecciona la petición a la KeyOne CA, mediante el módulo Servidor KeyOne CA Online. Es realmente, la KeyOne CA, quien lleva a cabo la certificación solicitada y se genera un mensaje de respuesta que es devuelto a la KeyOne LRA. Una vez que el supuesto certificado ha sido emitido, se incluye en el mensaje de respuesta, para que KeyOne LRA pueda entregarlo al subscriptor dentro de una tarjeta inteligente.

Un subscriptor del servicio de revocación hace una petición de suspensión, reactivación o revocación a la KeyOne LRA, que una vez verificada la identidad del mismo, redirecciona la petición a la KeyOne CA, mediante el módulo servidor KeyOne CA online. Es realmente, la KeyOne CA, quien lleva a cabo la suspensión o revocación solicitada y se genera un mensaje de respuesta que es devuelto a la KeyOne LRA.

Transacciones KeyOne LRA – KeyOne CA

Los servicios de revocación, generación de certificados y registro requieren una comunicación entre la KeyOne LRA y KeyOne CA. Los mensajes que se intercambian durante este proceso de comunicación se denominan lotes y cumplen con una sintaxis específica, que incluye la firma electrónica.

Además, estos mensajes se transfieren mediante una conexión SSL. Por lo tanto, la confidencialidad, autenticidad e integridad de las transacciones entre KeyOne CA y KeyOne LRA están garantizadas.

Los lotes se pueden clasificar en dos categorías, dependiendo del tipo de petición que contengan:

- Lotes CR: son lotes que contienen una petición de certificación.
- Lotes RR: Lotes que contienen una petición de revocación, suspensión o reactivación.
- Lotes UR: Lotes que contienen información sobre la petición, como por ejemplo, una petición de actualización de CRL o un fichero de configuración de LRA para instalar.

Servicio de Estado de Revocación

Un subscriptor del servicio de consulta de estado de revocación envía una petición OCSP al servidor KeyOne VA para determinar el estado de revocación de un certificado en concreto. A continuación, el Servidor KeyOne genera un mensaje de respuesta OCSP, después de consultar su base de datos interna, y la devuelve al subscriptor, quién procederá en consecuencia, cuando reciba dicha respuesta. Además, tanto los mensajes OCSP de entrada como de salida son registrados en la base de datos interna del Servidor KeyOne, para hacer posible las auditorías posteriores.

Servicio de Sellado de Tiempo

Un subscriptor del servicio de sellado de tiempo realiza la firma electrónica de unos datos y manda una petición de sellado de tiempo al servidor KeyOne TSA, de acuerdo a la sintaxis definida en la RFC 3161. Después, el servidor KeyOne TSA,



consigue la hora actual de un reloj seguro, y asocia ambos, la firma de los datos y el instante de tiempo en que se realizó, emitiendo el correspondiente indicador de sello de tiempo. Finalmente, este indicador se encapsula en un mensaje de respuesta TSP y se devuelve al subscriptor.

El indicador de sello de tiempo es una prueba de existencia de los datos fechados, y es una evidencia infalsificable, de que los datos existían antes de un determinado momento en el tiempo. Tanto los mensajes OCSP de entrada como de salida son registrados en la base de datos interna del Servidor KeyOne, para hacer posible las auditorías posteriores.

Arquitectura Física

La siguiente figura muestra los componentes incluidos en la arquitectura física del KTS:

Figura 2.5:Arquitectura Física del KTS

Todos los componentes KeyOne (excepto el componente KeyOne LRA) están conectados a una Base de Datos, donde se almacena toda la información relativa

al servicio. La base de datos del componente KeyOne CA almacena los certificados y CRL's generados, los lotes KeyOne (los lotes contienen grupos de peticiones de certificación o revocación, o certificados, depende de la entidad que los emita. El principal propósito de usar lotes en KeyOne es el envío de peticiones de revocación y certificación y la recepción de respuestas entre la LRA y la CA, y los registros de auditoría generados por el Servidor KeyOne. La base de datos asociada al componente KeyOne VA almacena los estados de los certificados, los mensajes intercambiados con el componente KeyOne CertStatus (parte del producto KeyOne), y los registros de auditoría generados por KeyOne Server.

Todos los componentes KeyOne (excepto el componente LRA) están conectados a un HSM (Módulo de seguridad Hardware), para generar y almacenar las claves asociadas al servicio, y también están conectados a un reloj que proporciona sellos de tiempo fiables ara ser usados por el propio servicio.

En el componente KeyOne LRA, un usuario puede solicitar la generación de un certificado (generación de las claves en una tarjeta inteligente) o el cambio de estado de un certificado generado previamente. En cuyo caso, el Operador de Registro, verifica la identidad de la entidad solicitante, y aprueba o deniega la petición, firmándola con el certificado de firma almacenado en una tarjeta inteligente. Una vez que el Operador de Registro firma la petición, entonces sse envía dentro de un lote KeyOne al servidor de KeyOne CA. Este servidor procesa la petición (cambia el estado del certificado en la base de datos de KeyOne CA o genera el certificado) y se envía el resultado a l servidor KeyOne LRA, dentro de otro lote. Si la solicitud implica la generación de un certificado, entonces éste se almacenará en la tarjeta inteligente del subscriptor.

KeyOne CA (el servidor KeyOne CertStatus) accede a la base de datos de KeyOne CA, donde se almacena la información del estado de revocación del certificado. Tanto ahora como antes, KeyOne VA enviará peticiones a KeyOne CA (al servidor KeyOne CertStatus) para obtener la lista de certificados que han cambiado de estado en el último intervalo de tiempo. NDCCP (*Near Domain Cert-status Coverage Protocol*) es un protocolo propietario de KeyOne, que se usa para la comunicación entre un módulo actualización de la base de datos (en KeyOne VA) y un módulo servidor CertStatus (en KeyOne CA).

El servidor KeyOne VA (la autoridad de validación) implementa el protocolo de Estado de Certificado *Online* (OCSP) y determina el estado actual de un certificado digital. Las partes de Confianza, usan este servicio para hacer peticiones del estado de los certificados a la Autoridad de Validación.

Los componentes del entorno para cada uno de los componentes KeyOne se listan en la tabla siguiente:

Subsistema	**SO**	**Base de Datos**	**HSM**	**SCD/SSCD**	**Reloj**	**Otros**
KeyOne CA	Microsoft Windows 2000	Oracle 9i	nCipher nShield Ultrasign 1.82.7		Time&Frequency Solutions. Modelo: NTP8. Firmware version: 0123NT-	Microsoft Internet Explorer 6.0 LDAP Netscape 4.0



					P v11.00	
KeyOne LRA	Microsoft Windows 2000			GPK 16000		Microsoft Internet Explorer 6.0 Gemplus GemPC410 Reader
KeyOne VA	Microsoft Windows 2000	Oracle 9i	nCipher nShield Ultrasign 1.82.7		Time&Frequency Solutions. Modelo: NTP8. Firmware version: 0123NT-P v11.00	Microsoft Internet Explorer 6.0
KeyOne TSA	Microsoft Windows 2000	Oracle 9i	nCipher nShield Ultrasign 1.82.7		Time&Frequency Solutions. Modelo: NTP8. Firmware version: 0123NT-P v11.00	Microsoft Internet Explorer 6.0

Tabla 2.2. Componentes de entorno

El Navegador de Internet debe proporcionar funcionalidad de Cifrado Fuerte (128 bits). Este requisito se satisface usando los productos de Microsoft Internet Explorer 6.0.

Casos de Uso

La funcionalidad del Objeto de Evaluación presentada en este documento puede resolver una gran cantidad de casos de negocio, desde la identificación de usuarios y el control de acceso a los recursos internos, hasta el comercio electrónico, y muchos diversos sectores de mercado.

No obstante, los servicios de seguridad que proporciona el KTS se pueden resumir en los siguientes:

1 Autenticación de Aplicación / Entidad / Usuario

2 Cifrado de la Información

3 No repudio e integridad, proporcionado por la firma digital avanzada.

Por lo tanto, cualquier aplicación o negocio que requiera alguno de los servicios de seguridad mencionados anteriormente, es capaz de usar un KTS.

El uso de este Objeto de Evaluación es más indicado en determinados esquemas de registro. Esta configuración se adapta perfectamente a:

- Entornos de registro distribuido, dada la facilidad y rapidez de distribución de diferentes LRAs, sin que exista un incremento de las necesidades de mantenimiento.

- Registros móviles o ambulantes, garantizando la seguridad del servicio de registro sin medidas de protección física muy restrictivas.

CAPÍTULO 3

Entorno de Seguridad del TOE

Hipótesis de Uso del Objeto de Evaluación

En general, el Objeto de Evaluación consistirá en una solución global de Proveedor de Servicios de Certificación, con su propio hardware, software y sus respectivas prácticas, procedimientos y políticas de seguridad, que se comunica a través de sus interfaces lógicos y físicos con las aplicaciones cliente, garantizando la prestación de estos servicios de la forma debidamente autorizada.

Desde un punto de vista lógico, es responsabilidad del Objeto de Evaluación proporcionar un amplio abanico de servicios de seguridad, que serán necesarios para la correcta securización de las aplicaciones o transacciones críticas, que así lo requieran.

- Identificación y autenticación, garantiza que los datos del emisor y receptor serán identificados de forma unívoca, de tal forma que ambas partes conozcan la procedencia y el destino de dicha información.
- Confidencialidad, garantiza que la información está protegida frente a accesos no autorizados
- Integridad de datos, garantiza que los datos no han sido modificados de forma accidental o deliberada.
- No Repudio, proporciona evidencias de la integridad y de la procedencia de la información, que pueden ser verificada por una tercera parte

El conjunto de políticas establece las garantías de seguridad que un Proveedor de Servicios de Certificación necesita cumplir y las prácticas y procedimientos a seguir para alcanzar y mantener dichas garantías.

Los principales supuestos considerados en el entorno, que ayudan al cumplimiento de las políticas de seguridad definidas, son las siguientes:

H1. SEGURIDAD FÍSICA Y DEL ENTORNO

El acceso físico a los servicios críticos está controlado y los riesgos de acceso físico a sus activos han sido minimizados. En concreto, el acceso físico a los servicios de generación de certificados, Suministro de dispositivos de usuario y los de gestión de revocación se limitará al personal debidamente autorizado.

Estas salvaguardas comprenden todos aquellos mecanismos de seguridad no informáticos, como son la seguridad física, seguridad en el personal, seguridad en los procedimientos.



H2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Se establecerá, documentará, implementará y mantendrá una Política de Seguridad del Sistema, que identifique todos los objetivos relevantes, objetos y amenazas potenciales relativas a los servicios proporcionados y las medidas de salvaguarda requeridas para evitar o limitar los efectos de dichas amenazas. Se recomienda que la documentación describa las reglas, directrices y procedimientos necesarias para garantizar los servicios y las propiedades de seguridad especificadas, junto con la definición de una política de actuación frente a incidentes y desastres.

H3. DESARROLLO Y MANTENIMIENTO DEL TWS

Se llevará a cabo una análisis de requisitos de seguridad en las fases de diseño y especificación de requisitos de todo proyecto de desarrollo de sistemas soportado por KeyOne TWS o mediante KeyOne TWS, de forma que se garantice que la seguridad está imbuida dentro del sistema informático y los riesgos de fallo del sistema han sido minimizados.

En particular, existirán procedimientos de control de cambios para nuevas versiones, modificaciones y parches que vaya saliendo en el software de operación.

H4. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO Y GESTIÓN DE INCIDENTES

El sistema fiable KeyOne garantizará, en caso de desastre, y siempre que las claves privadas de firma del TWS KeyOne se vean comprometidas, la restauración de la operación del sistema tan pronto como sea posible.

Particularmente, el plan de continuidad del negocio de la TWS KeyOne (o plan de recuperación ante desastres) contemplará el compromiso o supuesto compromiso de las claves privadas de firma del TWS KeyOne.

H5. CUMPLIMIENTO DE LOS REQUERIMIENTOS LEGALES

El TWS KeyOne asegurará el cumplimiento de los requerimientos legales aplicables:

i. Los registros serán protegidos frente a pérdida, destrucción y falsificación. En algunos casos, puede hacerse necesaria, la conservación de los mismos para cumplir disposiciones reglamentarias, así como para servir de apoyo a las actividades principales del negocio.

ii. El TWS KeyOne deberá asegurar el cumplimiento de los requisitos de la Directiva Europea de Protección de Datos, en su transposición a la normativa española (LO 15/1999, RD994/1999)

iii. Se tomarán medidas organizativas y técnicas frente al procesamiento de datos personales no autorizado o fraudulento y pérdidas o destrucción accidentales, o cualquier daño a este tipo de datos.

La información que los usuarios proporcionan al TWS KeyOne, será protegida frente a revelaciones no autorizadas, siempre que no existan un acuerdo de usuario, una órdenes judiciales u otro documento legal que lo autorice.

H6. POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN

Se deben definir políticas específicas para la gestión de certificados cualificados, de conformidad con [TS1] y las Políticas de Requisitos de Seguridad CWA [CEN01c], así

como las prácticas de certificación que ponen en marcha estas políticas, para asegurar la confiabilidad de la operación del TWS KeyOne.

La Política y Declaración de Prácticas de Certificación son documentos habitualmente empleados para la definición de estas políticas dentro del entorno del Proveedor de Servicios de Certificación. A tal fin, también se aporta como Anexo una guía de soporte a la documentación de la CPS KeyOne 2.1, para la elaboración de la documentación de Políticas y Prácticas de Certificación, conforme a esta Declaración de Seguridad.

H7. COMPETENCIA DEL PERSONAL

El personal involucrado en la operación y administración del Objeto de Evaluación será de confianza y competente para desarrollar sus funciones con la debida diligencia, evitando cualquier uso incorrecto de las funciones y equipos del Objeto de Evaluación.

H8. PROGRAMA DE CAPACITACIÓN Y CONCIENCIACIÓN

Se deberá establecer y mantener un programa de formación y concienciación efectivo. Será requerida la aceptación y participación de todo el personal dentro de la organización de la PKI, para lograr el conocimiento adecuado y estar informado de la existencia y el alcance de las medidas, prácticas y procedimientos para la seguridad del sistema de información del Objeto de Evaluación.

Para una correcta implementación de todos los requisitos de seguridad del Objeto de Evaluación, identificados en este documento, es fundamental un programa de formación. Operadores y administradores del Objeto de Evaluación tienen que conocer todas las implicaciones de seguridad que conllevan sus obligaciones, y cuáles son las mejores prácticas para acometer sus tareas, que vendrán indicadas en la documentación de instalación y configuración del producto, así como en la CPS KeyOne 2.1.

H9. FUENTE DE TIEMPO FIABLE

Se deberá seleccionar e implementar una fuente de tiempo fiable y de confianza, que dé soporte a los procesos relativos al tiempo de la gestión del ciclo de vida de los certificados.

Por otro lado, el Sellado de Tiempo, depende de la autenticidad del reloj que se usa. Por lo tanto, los usuarios del Objeto de Evaluación necesitan un servicio de sellado de tiempo que emplee un reloj con altos requerimientos de fiabilidad, disponibilidad y confiabilidad.

Es importante que los relojes internos de los equipos estén correctamente configurados para garantizar la exactitud de los registros de auditoría. Estos registros pueden ser requeridos para investigaciones o como evidencias en procesos legales o disciplinarios. Unos registros de auditoría inexactos pueden entorpecer las investigaciones y dañar la credibilidad de tales evidencias.

Si un ordenador o dispositivo de comunicaciones tiene la capacidad de estar operando un reloj de tiempo real, éste debe ajustarse con un estándar acordado, como por ejemplo *Universal Co-ordinated Time* (UTC) o un tiempo estándar local. Puesto que algunos relojes pueden desviarse en el tiempo, debe haber un procedimiento que compruebe y corrija cualquier variación significante.



H10. MÓDULO DE SEGURIDAD HARDWARE (HSM)

Se debe usar protección física, a la hora de proteger los procesos de generación y archivado de claves secretas frente a modificación, destrucción y revelación, en cumplimiento de [CEN CMCSO-PP].

H11. DISPOSITIVOS SEGUROS DE CREACIÓN DE FIRMA

La inicialización, formateado, y creación de la estructura de ficheros vendrá predefinida por el fabricante de tarjetas, en la fase de preparación del SSCD, en la que se obtendrá una configuración segura con un PIN por defecto. Este PIN se cambiará vía procedimientos de registro con el fin de crear los datos de activación iniciales de una forma segura, tal y como se describe en los procedimientos de configuración para salvaguardar su integridad y confidencialidad.

H12. MECANISMOS DE CONTROL DE ACCESO

Se usarán los servicios de seguridad que proporciona el sistema operativo, para restringir el acceso a los equipos y recursos de información críticos. Estos servicios deberán ser capaces de:

- Proteger la información residual sensible, que pueda quedar almacenada en ficheros temporales, borrándolos o desactivando este tipo de funcionalidades.
- Restringir el acceso a las bases de datos del sistema y otras aplicaciones, que puedan usarse para evitar los mecanismos de seguridad establecidos por el Objeto de Evaluación.

Activos a proteger

Basándonos en un análisis de vulnerabilidades específico para este tipo de infraestructuras, se puede obtener los principales activos a proteger y clasificarlos en función de sus necesidades de garantía de seguridad.

Confidencialidad

La confidencialidad cubre los datos almacenados, la información generada durante su procesamiento y la que se comunica. El acceso a la información confidencial por el personal de operación está basada en una necesidad de conocer.

A.1 Información de Registro

Toda la información registrada por el servicio de registro es información confidencial, incluyendo:

1. Las Solicitudes de Certificación, tanto aprobadas como rechazadas;
2. Información de certificación recopilada como parte de la información de registro, siempre que ello no impida la publicación de la información del certificado en un directorio X.500, en cumplimiento de la ley de protección de datos.

A.2 Información del Certificado

El motivo por el cuál, un certificado es suspendido o revocado se considera información confidencial, con la excepción de que la revocación de un certificado del proveedor de servicio se deba a las siguientes causas:

1. El compromiso de sus claves privadas, en cuyo caso puede revelarse que la clave privada ha sido comprometida.
2. La finalización de la actividad del proveedor del servicio, en cuyo caso se puede notificar previamente la terminación del mismo.

A.3 Clave Criptográficas

La gestión de las claves privadas y/o secretas debe hacerse de forma segura. En función de las distintas amenazas a las claves de los TWSs, y dependiendo de dónde y cómo se usen, es importante clasificar las claves de acuerdo a su perfil de riesgo. En esta especificación, las claves se han clasificado en las siguientes categorías:

i. Claves de firma de QC/NQC – El par de claves del Servicio de Generación de Certificado usados para la emisión de Certificado Cualificados o No-Cualificados y claves para firmar la información del estado del certificado. En términos de requisitos de seguridad, las claves de firma de QC/NQC son claves de larga duración, cuyo impacto debido a la exposición es alto. Por tanto, las contramedidas para gestionar este riesgo son fuertes, tanto en número como en efecto.

ii. Claves de Infraestructura. Estas son las claves usadas por los TWSs, para procesos como acuerdo de claves, autenticación de subsistema, firmado de registro de auditoría, cifrado de los datos almacenados o transmitidos, etc. Las claves de sesión, por su corta duración, no entran dentro de esta categoría. Estas claves se consideran también de alto riesgo, pero dado que su funcionalidad está distribuida y su período de validez es menor, son de menor riesgo, en comparación a las claves de firma.

iii. Claves de Control. Estas son las claves usadas por el personal que gestiona y opera con el TWS y pueden proporcionar servicios de autenticación, firma o confidencialidad al personal que interacciona con el sistema. Las claves de menor riesgo, usadas por los TWSs del Proveedor de Servicio de Certificación, son aquellas usadas por el personal que controla los TWSs, ya que son usadas por individuos de confianza, y su periodo de validez es aún más corto.

iv. Las claves de sesión, que se usan para transacciones simples/cortas son tratadas como información sensible pero con unos requisitos de seguridad menores que las categorías definidas anteriormente.

A.4 Módulo de Seguridad Hardware

Las claves privadas o secretas usadas para la firma de certificados, CRLs u otras declaraciones sobre el estado de los certificados, deberán almacenarse en



dispositivos resistentes a la manipulación y protegidos frente a usos no autorizados o copias.

Integridad

La integridad de los datos es la característica que previene de que los datos sean alterados de forma no autorizada, ya sean datos almacenados, datos de procesamientos o datos de intercambio.

A.5 Información de intercambio (Peticiones/Respuestas)

La información sensible intercambiada a través de los interfaces externos e internos del Objeto de Evaluación de forma *on-line*, *off-line* u otros medios de comunicación físicos, deberá ser protegida frente a modificaciones, interrrupciones y bloqueos.

A.6 Código Fuente, Datos de Configuración e Información de Auditoría

Deben existir mecanismos para verificar la integridad de las aplicaciones del Objeto de Evaluación frente a modificaciones no autorizadas.

A.7 Fuente de Tiempo

Se requieren fuentes de tiempo fiables, no sólo para proporcionar un servicio de sellado de tiempo confiable, sino también para disponer de registros de auditoría precisos y oportunos.

Disponibilidad

La protección contra ataques accidentales o intencionados de denegación de datos del servicio, que impidan el acceso autorizado a los recursos o demoren las operaciones críticas en el tiempo.

La disponibilidad de determinados servicios en tiempo real es crítica, ya que deben proporcionar un servicio puntual, como son:

A.8 Servicios de Gestión de Revocación

La revocación del certificado es el mecanismo utilizado para invalidar un certificado y su correspondiente asociación de clave, cuando se ha detectado o se sospecha la existencia de un compromiso de la clave privada. Por ello, se requiere una respuesta puntual que asegure cualquier falsificación potencial, invalidando la confianza en el certificado digital usado para verificar la identidad del propietario de la clave privada.

A.9 Servicios de Estado de Revocación del Certificado

Una vez que se procesa una solicitud de revocación, el nuevo estado del certificado debe ser distribuido oportunamente, por el servicio de estado de revocación de certificado, a las partes confiables.

A.10 Servicio de Sellado de Tiempo

La calidad de este servicio depende mucho de que la fuente de tiempo sea fiable, de su exactitud y de su disponibilidad para proporcionar unos sellos de tiempo de confianza.

Amenazas de Seguridad

Las amenazas más comunes a este tipo de infraestructuras se centran en romper la necesaria confianza y fiabilidad de los servicios del Objeto de Evaluación, mediante violaciones potenciales de la integridad, confidencialidad o disponibilidad de los activos del Objeto de Evaluación.

T1. Violación de las políticas de seguridad y de las prácticas de certificación del TOE

Los usuarios del Objeto de Evaluación dejan de hacer algunas de las funciones esenciales para la seguridad, modificando los datos del TSF de forma inconsistente con las políticas de seguridad de la información y las prácticas de certificación, con la consiguiente revelación o modificación de las claves privadas y secretas. Estas acciones adversas pueden dañar las propiedades de seguridad de los siguientes activos: A.1, A.2, A.3, A.4, A.5, A.6, A.7, A.8, A.9, A.10.

T2. Violación del código

Los usuarios del Objeto de Evaluación pueden explotar sus vulnerabilidades o agujeros de seguridad, derivados de los procesos de ingeniería del software que no han sido identificados a tiempo. Esta amenaza podría generar procesos irregulares que violen la integridad, disponibilidad, o confidencialidad de los activos del sistema, como A.1, A.2, A.3, A.5, A.6, A.7, A.8, A.9, A.10

T3. **Ataques externos**

Un *hacker* puede acceder al sistema usando ingeniería social o haciéndose pasar por un usuario autorizado a realizar operaciones que se atribuirían al usuario o proceso del sistema autorizados.

Un *hacker* puede modificar información interceptada a través de las líneas de comunicación entre dos entidades, antes de llegar al destino previsto y puede causar denegación de servicios críticos.

Los activos potenciales que pueden quedar comprometidos debido a este ataque son los siguientes: A.1, A.2, A.3, A.4, A.5, A.6, A.7, A.8, A.9, A.10.

Políticas de Seguridad Organizativa

Las siguientes políticas de seguridad organizativa son una descripción detallada de algunos de los requisitos de política establecidos para sistemas de gestión de certificados para firmas electrónicas conforme a los Sistemas de confianza tal y como se describe en el Anexo (f) de [Eur99b].

Serán implementadas por el Objeto de Evaluación y el entorno como se identificó en los supuestos y políticas y prácticas descritas en el Apéndice CPS de KeyOne 2.1.



Estas políticas se clasifican en dos grandes grupos, el primero es aplicable a todos los servicios del Prestador de Servicios de Certificación, y el segundo es específico para cada servicio:

Políticas Generales

Son aplicables tanto para los servicios básicos como para los suplementarios.

P.SO – Sistemas y Operaciones

P_SO1.1 Gestión de las Operaciones

Un Proveedor de Servicios de Certificación que opera con sistemas fiables necesita garantizar que las funciones de gestión de dichas operaciones son lo suficientemente seguras.

Se deben proporcionar las instrucciones del fabricante del sistema fiable, necesarias para permitir que el sistema:

1. Opere de forma correcta y segura;
2. Se construya de forma que se minimice el riesgo de fallos del sistema;
3. Esté protegido frente a virus y software malicioso para asegurar que se mantiene la integridad de los sistemas y de la información que procesa.

P_SO3.1 Sincronización del tiempo

La emisión de certificados y su posterior gestión es dependiente del tiempo, por lo que existe una necesidad de garantizar que los sistemas fiables están adecuadamente sincronizados a una fuente de tiempo estándar. Este requisito es independiente de los requisitos del sellado de tiempo, que debe poner en marcha el Proveedor de Servicios de Certificación.

Se debe indicar la precisión del tiempo y todos los relojes del TWS deben sincronizarse en un intervalo de 1 segundo de *Co-ordinated Universal Time*.

P.IA - Identificación y Autenticación

Las funciones de identificación y autenticación controlan el uso y el acceso de los Sistemas Fiables, sólo a personal autorizado. Abarcan todos los componentes de gestión del Proveedor de Servicios de Certificación. Esta Identificación y Autenticación, puede ser proporcionada por el sistema operativo o directamente por el propio componente.

P_IA1.1 Autenticación de Usuario

Los Sistemas Fiables solicitarán la identidad de cada usuario y su correcta autenticación antes de permitir cualquier acción derivada del usuario o rol asignado al mismo.

P_IA1.2 Re-autenticación de Usuario

Es obligatoria la re-autenticación del usuario una vez que abandone el sistema.

P.KM – Gestión de Clave

Un sistema Fiable utilizará claves criptográficas para proporcionar funciones de integridad, confidencialidad y autenticación dentro de sus propios subsistemas y entre ellos. Como tal, el uso, revelación, modificación o sustitución provocará una pérdida de la seguridad del Sistema Fiable KeyOne. Es fundamental, que toda la gestión del ciclo de vida de las calves secretas o privadas se lleve a cabo de forma segura.

Las claves de Infraestructura y de Control pueden ser tanto asimétricas como simétricas.

Generación de Claves

La Generación de claves se refiere a la creación de las claves.

KM1 Generación de Clave

P_KM.1.1

Las claves de firma de QC/NQC se generan y almacenan en módulos criptográficos seguros.

P_KM.1.3

El modulo criptográfico seguro sólo genera claves de firma de QC/NQC bajo el control de mínimo dos personas.

P_KM.1.4

Las claves de Infraestructura y Control se generan y guardan en dispositivos criptográficos hardware (HCD).

P_KM.1.7

La generación de claves cumplirá los requisitos criptográficos especificados en [ALGO], que le sean de aplicación.

Distribución de Claves

La distribución de claves es la función de distribuir las claves de Control, de Infraestructura o las claves públicas de QC/NQC del Servicio de Generación de Certificados.

P_KM.2.1

Las claves secretas y privadas no se distribuyen en claro.

P_KM.2.2

Las claves públicas que no han sido certificadas se guardan de forma segura para prevenir interceptaciones o manipulaciones.



P_KM.2.3

El sistema KeyOne distribuye las claves criptográficas siguiendo un método de distribución de clave criptográfica específico.

P_KM.2.4

La clave pública asociada a las claves de firma de QC y/o las claves de Infraestructura (como por ejemplo, el Servicio de Estado de Revocación, el Sellado de Tiempo), tiene que estar accesibles a los usuarios y parte de confianza. La integridad y autenticidad de dichas claves públicas y sus parámetros asociados se mantiene en su inicial y sucesivas distribuciones.

P_KM.2.5

Un certificado auto-firmado generado por la KeyOne CA cumple las siguientes propiedades:

- La firma del certificado puede ser verificada con los datos proporcionados dentro del certificado;
- Los campos sujeto y emisor del certificado son idénticos.

P_KM.2.6

El sistema KeyOne puede generar una huella digital de un certificado auto-firmado mediante los algoritmos de *hash* definidos en [ALGO].

Uso de la Clave

Consiste en el control del uso de las claves generadas mediante algoritmos criptográficos para proporcionar servicios criptográficos.

P_KM.3.1

Todos los módulos criptográficos seguros tienen mecanismos de control de acceso para las claves de Control, Infraestructura y firma de QC/NQC

P_KM.3.4

Los Sistemas fiables que proporcionan Servicios de Suministro de Dispositivos de Usuario, DEBEN garantizar que las claves de usuario para la creación de las firma electrónicas son independientes de las que se usan para otras funciones como el cifrado.

Advertencia: Los Sistemas Fiables asegurarán que la extensión "uso de la "clave" esté presente en los certificados de firma usados. Si el bit de no-repudio está activado, entonces NO DEBERÍA combinarse con otros usos de clave, por ejemplo, el bit de no repudio, cuando se use se hará de forma exclusiva.

P_KM.3.5

Sólo se podrá hacer un uso autorizado de la clave, durante su periodo de validez (como determine la política).

P_KM.3.6

El sistema KeyOne confía en los certificados de claves asimétricas de Control o de Infraestructura, una vez que se asegura de que los certificados asociados son aún válidos.

Cambio de Clave

El cambio de Clave puede ser:

- Programado – cuando una clave es reemplazada por una nueva, al vencimiento de la validez de la misma (como se determine en la política);
- No-Programado – cuando una clave es reemplazada por otra nueva, si ha sido comprometida.

P_KM.4.1

Las claves de Control e Infraestructura deberán cambiarse regularmente, por ejemplo anualmente.

Advertencia: cuando alguno de los algoritmos usado por el sistema KeyOne pasen a ser considerados no aptos (como se especifique en [ALGO]), las claves basadas en estos algoritmos se cambiarán inmediatamente.

P_KM.4.2

El cambio de claves se llevará de forma segura y mediante mecanismos fuera de línea.

Destrucción de clave

Cuando se compromete una clave o finaliza su periodo de validez, puede ser destruida para prevenir un uso futuro de la misma.

P_KM.5.1

Cuando las claves de firma de QC/NQC caducan, son destruidas de forma que no puedan ser recuperadas.

P_KM.5.2

Cuando los sistemas que se han usado para la generación, uso o almacenamiento de claves privadas/secretas vayan a ser retirados, sus claves asociadas serán destruidas.

Almacenamiento, Copia y Recuperación de Clave

Después de ser generadas, las claves pueden ser almacenadas en entornos seguros y ser copiadas y salvaguardadas para cumplir requisitos operacionales. Dichas copias de seguridad de las claves podrán ser recuperadas en casos, por ejemplo, de borrado involuntario de las mismas.

P_KM.6.1

Todas las claves privadas/secretas son almacenadas de forma segura.



P_KM.6.3

Las claves privadas/secretas de Control y de Infraestructura son almacenadas en dispositivos Criptográficos Hardware (HCD).

P_KM.6.4

Toda clave privada/secreta almacenada en un módulo criptográfico seguro o HCD, que va a ser exportado, es protegido por el módulo, para garantizar su confidencialidad antes de almacenarse fuera del módulo. Cualquier material de claves sensible, nunca será almacenado de forma desprotegida.

Advertencia: Cuando la clave Privada/Secreta sea protegida mediante cifrado, se cumplirán los requerimientos criptográficos especificados en [ALGO].

P_KM.6.5

El sistema KeyOne garantiza que la copia de seguridad, almacenamiento y restauración de las claves privadas de Control, Infraestructura y de firma de QC/NQC, sólo se realiza por personal autorizado.

P_KM.6.6

El sistema KeyOne garantiza que la copia de seguridad, almacenamiento y restauración de las claves privadas de firma de QC/NQC sólo se realiza mediante control dual.

P_KM.6.7

El sistema KeyOne no dispone de funciones que permitan hacer copias de seguridad o recuperar las claves de firma de usuario (claves privadas).

Archivado de Clave

Cuando la clave caduca, puede ser archivada, para permitir el uso de la misma posteriormente. Especialmente, cuando se refiere a las claves públicas usadas en la verificación de firmas electrónicas, pero esto no excluye que se archiven otro tipo de claves, siempre que se justifique.

P_KM.7.1

El sistema KeyOne no contiene funciones que permitan el archivado de las claves de firma de usuario (claves privadas).

P.AA – Responsabilidad y Auditoría

Se deben proporcionar de forma segura, datos de registro de evidencias de las actividades de operación del Sistema Fiable. Los registros deben ser completos, y estar disponibles para las entidades autorizadas.

Cada servicio tendrá otros requerimientos específicos de auditoría, que deben considerarse además de estos requisitos generales.

AA2 Garantías de Disponibilidad de los datos de auditoría

P_AA.2.2

Los datos de auditoría no serán sobrescritos de forma automática.

AA3 Parámetros de los Datos de Auditoría

P_AA.3.1

Todos los registros de auditoría (incluso los registros de auditoría propios del servicio) DEBEN contener los siguientes parámetros:

- Fecha y Hora del evento;
- Tipo de Evento;
- Identidad de la entidad responsable de la acción;
- Acierto o fallo del evento auditado.

AA4 Revisión de Auditoría Seleccionable

P_AA.4.1

Todos los componentes KeyOne ofrecen la posibilidad de búsqueda de eventos en los registros de auditoría, en función de la fecha y hora del evento, tipo de evento y/o identidad del usuario.

P_AA.4.2

El TSF proporcionará los registros de auditoría de forma adecuada para que el usuario pueda interpretar la información.

AA5 Revisión de Auditoría Restringida

P_AA.5.2

Se prevendrán las modificaciones a los registros de auditoría.

AA7 Garantías de la Integridad de Datos de Auditoría

P_AA.7.1 – SOLO QC

El sistema KeyOne garantiza la integridad de los datos de auditoría. El sistema KeyOne también proporciona una función para verificar la integridad de los datos de auditoría.

AA8 Garantías del Tiempo de la Auditoría

P_AA.8.1

Para marcar el tiempo de los eventos auditados se utiliza una fuente de tiempo fiable.



P.AR – Archivado

Se debe generar y mantener un archivo seguro en un soporte apropiado para almacenamiento y posterior procesamiento de las evidencias legales necesarias para dar soporte a las firmas electrónicas.

AR1 Generación de Datos de Archivo

P_AR.1.1

El sistema KeyOne es capaz de generar un archivo en soporte apropiado para el almacenamiento y posterior procesado de las evidencias legales necesarias para dar soporte a las firmas electrónicas.

P_AR.1.2

Como mínimo, los siguientes elementos serán archivados:

- Todos los certificados;
- Todas las CRLs/ARLs;
- Todos los registros de auditoría.

P_AR.1.3

Cada entrada incluye el tiempo en el que ocurrió el evento.

P_AR.1.4

El archivo no incluye parámetros críticos para la seguridad de forma no protegida.

AR2 Búsqueda Seleccionable

P_AR.2.1

El sistema ofrece la posibilidad de búsqueda de eventos en el archivo, en función del tipo de evento.

AR3 Integridad de los Datos Archivados

P_AR.3.1

Cada entrada en el archivo está protegida frente a modificaciones.

P.BK – Copias de Salvaguarda y Recuperación

Las copias de salvaguarda y recuperación del sistema de información del Objeto de Evaluación, la información del usuario y otros datos necesarios para restaurar el sistema después de un fallo o desastre. Esto no incluye la copia y la recuperación de claves, cuyos requisitos de seguridad se encuentran en la sección de Almacenamiento, Copia y Restauración de claves.

BK1 Generación de Copias de Seguridad

P_BK.1.1

El sistema KeyOne incluye una función de copia de seguridad.

P_BK.1.2

Los datos almacenados en la copia de seguridad son suficientes para recuperar el estado del sistema.

P_BK.1.3

Un usuario que tenga un rol con los suficiente privilegios, es capaz de invocar la función de copia de seguridad a demanda.

BK2 Integridad y Confidencialidad de Información de Copias de Seguridad

P_BK.2.1 – SOLO QC

Las copias de seguridad están protegidas frente a modificaciones mediante el uso de firmas digitales, funciones *hash* o códigos de autenticación.

P_BK.2.2

Los parámetros críticos para la seguridad y demás información confidencial es almacenada sólo de forma cifrada. El cifrado cumple con los requerimientos especificados en [ALGO].

BK3 Recuperación

P_BK.3.1

El sistema incluye funciones de recuperación capaces de restablecer el estado del sistema desde una copia de seguridad.

P_BK.3.2

Un usuario que tenga un rol con los suficiente privilegios, es capaz de invocar la función de recuperación a demanda

P. SM –Mensajes Seguros Generales

GE1 General

P_GE.1

Todos los mensajes generados por un servicio básico:

- Son protegidos (p. ej. Mediante códigos de autenticación de mensajes, firmas electrónicas, etc.) mediante las claves de infraestructura del servicio;
- Contienen información del tiempo, para indicar cuándo creó el mensaje el emisor;
- Incluyen protección frente a ataques de repetición (p.ej. usando *nonces*)



Políticas de Servicio específicas

Este conjunto de políticas se aplica a cada servicio del Prestador de Servicios de Certificación, por lo que se agrupan por servicio. Se reflejarán en la documentación de Declaración de Prácticas de Certificación concreta.

P. RS – Servicio de Registro

Solicitud de Certificación

La Solicitud de certificación se lleva a cabo por el servicio de Registro, después de proceder a la identificación del usuario, de acuerdo a los requerimientos especificados en la Política de Certificación asociada, por ej. [TS1].

Gestión de Datos del Titular

El Servicio de Registro, por su naturaleza, debe gestionar datos de entidades finales. Estos datos están sujetos a distintos requisitos de protección de datos.

R1 Petición de Certificados

Un oficial de Registro verifica con los medios apropiados, de acuerdo con la legislación nacional, la identidad y, cuando sea aplicable, atributos específicos de la persona a la que se va a emitir el NQC/QC.

P_R.1.1

Siempre que la solicitud de certificación contenga información sensible del usuario, la petición de certificación se protegerá antes de ser enviada al Registro para la generación del certificado, de forma que se garantice la confidencialidad del mensaje. El sistema KeyOne garantiza que esta funcionalidad se proporciona cuando es requerida.

P_R.1.2

El servicio implementa un mecanismo para obtener una prueba de posesión (POP) que garantice que la entidad que solicita la certificación es el verdadero poseedor de la clave privada asociada a la clave pública a certificar.

P_R.1.3 – SOLO QC

El servicio de Registro está configurado para permitir reunir todos los datos del usuario necesarios para satisfacer los requerimientos para Certificados Cualificados, como se recoge en el Anexo I de [Eur99b].

P_R.1.4

El Sistema KeyOne proporciona un mecanismo para la aprobación de solicitudes de certificación, por un oficial de Registro, antes de abandonar el Servicio de Registro.

P_R.1.6

Las peticiones de certificación del Servicio de Registro, son electrónicamente firmadas para autenticación e integridad de las mismas, mediante sus claves de Control y de Infraestructura.

R2 Gestión de Datos de Usuario

P_R.2.1

El sistema KeyOne implementa mecanismos y controles de seguridad para proteger la privacidad y confidencialidad de la información de usuario.

R3 Auditoría del Servicio de Registro

P_R.3.1

Los siguientes eventos específicos del Servicio de Registro son registrados:

- Todos los eventos relacionados con el registro, incluyendo las peticiones de actualización de claves del certificado;
- Todos los eventos relativos a las peticiones aprobadas para certificación.

P.CGS –Servicio de Generación de Certificados

Generación de Certificados

Después de recibir una solicitud de certificación procedente del Servicio de registro, el sistema KeyOne genera un certificado con la clave pública suministrada. Esto garantiza que el Proveedor de Servicios de Certificación ha "bloqueado" la asociación de la clave pública del usuario a su identidad.

Continuando con la Generación del Certificado, el certificado debe ponerse a disposición ya sea mediante el Servicio de Diseminación, el servicio adicional de Suministro de Dispositivo de Usuario o directamente al usuario.

P_CG.1.1

El servicio de Generación de Certificados garantiza la integridad, la autenticidad del origen de los datos, cuando se necesita, la privacidad y confidencialidad del mensaje de petición de certificación.

P_CG.1.2

El mensaje es procesado de forma segura y su conformidad con la Política de Certificación aplicable, chequeada.

P_CG.1.3

Antes de la Generación del certificado, el sistema KeyOne garantiza que se valida la Prueba de Posesión.

P_CG.1.4 – SOLO QC

La clave usada para firma de QC sólo debe ser usada para la firma de QCs y, de forma opcional, los datos sobre el estado de revocación del mismo.

P_CG.1.6

Todos los certificados emitidos por el sistema KeyOne tienen las siguientes propiedades:



- Indicación del nombre de usuario o seudónimo.
- La clave pública del certificado está relacionada con la clave privada del usuario.
- La firma electrónica avanzada del Proveedor de sistemas de Certificación, creada mediante las claves de firma del CSP.
- Un nombre distinguido único y un número de serie asignados por KeyOne CA. Este es único con respecto al CSP emisor.
- El certificado especifica la fecha de inicio de la validez del mismo nunca anterior al momento actual y una fecha de finalización nunca anterior al de inicio de la validez.
- Los algoritmos/claves de firma utilizados por KeyOne CA para la firma de certificados son conformes a los estándares de especificación de algoritmos [ALGO].
- Una referencia a la Política de Certificación bajo la cuál se emite el certificado.

P_CG.1.6 – SOLO QC

Todos los Certificados cualificados emitidos por el sistema KeyOne son conformes con [TS101862].

Renovación de Certificado

Durante el periodo anterior al de expiración del certificado, el cual se define en lla política aplicable, el certificado puede ser renovado. La renovación del certificado consiste en la renovación de la clave: una nueva clave pública es certificada, con la información de registro utilizada para generar el certificado anterior.

P_CG.2.3

El sistema KeyOne garantiza que las claves de firma de QC/NQC son actualizados antes de su fecha de expiración. Las claves públicas renovadas proporcionan como mínimo el mismo nivel de confianza que cuando fueron inicialmente distribuidas.

Esto se lleva a cabo, proporcionando al menos los siguientes certificados intermedios que muestran la posesión de la nueva clave privada, del siguiente modo:

- Proporcionando un certificado de la clave pública antigua firmado con la nueva clave privada;
- Proporcionando un certificado de la nueva clave pública firmado con la antigua clave privada;
- Proporcionando el nuevo certificado auto-firmado (firmado con la nueva clave privada).

P_CG.2.4

El sistema KeyOne proporciona un mecanismo de renovación de claves de usuario, tan seguro como el proceso de generación inicial de certificado.

P.CRMS –Servicio de Gestión de Revocación de Certificado

RM1 Las peticiones de cambio de estado de certificado motivadas por que el usuario considera que sus claves privadas pueden estar comprometidas, una petición de suspensión de su certificado (revocación temporal) se envían al sistema fiable del CSP. La petición correspondiente para activar el certificado después de una suspensión puede hacerse por el usuario.

Cuando el usuario sabe realmente que su clave privada está comprometida, se envía una petición de revocación de su certificado al sistema fiable de su CSP.

El CSP también puede solicitar un cambio de estado de certificado mediante este servicio. Estas peticiones son mensajes autenticados y pueden ser aceptadas o rechazadas por el CSP.

P_RM.1.1

Las peticiones e informes relativas a la revocación y/o suspensión se procesan puntualmente. El tiempo máximo transcurrido entre que se recibe la petición de una revocación y/o suspensión, hasta que cambia la información sobre el estado del certificado, no excederá de un día (24 horas).

Advertencia: *Rauth* +MP < 24 Hrs, por lo que el sistema KeyOne es capaz de procesar peticiones dentro del intervalo *MP*.

Donde *Rauth* es el tiempo de autenticación de la revocación (por medios procedimentales o automáticos; *MP* es el tiempo de propagación del mensaje de revocación desde que sale del Servicio de Revocación hasta que llega al Servicio de Consulta del Estado de Revocación (Requisito del sistema KeyOne).

P_RM.1.2

Todas las peticiones de suspensión, reactivación y revocación son adecuadamente autenticadas y validadas.

P_RM.1.3

Una vez que el certificado es definitivamente revocado, el sistema KeyOne garantiza que no podrá ser reactivado de nuevo.

P_RM.1.4

La revocación de certificados de claves de firma de QC/NQC DEBE hacerse ÚNICAMENTE bajo al menos un control dual.

P_RM.1.6

La base de datos que contiene el estado de los certificados se actualiza inmediatamente después de completar el procesado de la petición/informe (*Rauth*).

RM2 Revocación/Suspensión de Certificados

El Sistema Fiable que recibe una petición de revocación o suspensión mediante este servicio, cambia el estado del certificado a Suspendido o Revocado en su Base de Datos de Estado de los Certificados, y ésta es, a su vez, utilizada por el Servicio de Estado de Revocación.



P_RM.2.2

Cuando se usa el sistema de mensajes periódicos, el sistema KeyOne soporta los siguientes requerimientos:

- Para un repositorio *offline* (p. ej. la CRL accesible mediante directorios), el Servicio de Estado de Revocación se actualiza al menos diariamente.
- Para un repositorio *online* (p.ej. OCSP responder) el servicio de estado de revocación se actualiza siempre que hay un cambio, y además, una vez al día.
- En cada mensaje de actualización se incluye el nombre y la firma digital del emisor del mensaje, y el momento del cambio de estado.
- Los mensajes indican qué certificados se han revocado/ suspendido.
- Para cada certificado de la lista, se indica su número de serie y la razón del cambio de estado, en el mensaje.

P_RM.3.1

Los siguientes eventos específicos del Servicio de Gestión de Revocación de Certificados DEBEN ser registrados:

Todos los eventos relativos a las peticiones de cambio de estado de certificado, se aprueben o no.

P. CRSS – Servicio de Estado de Revocación del Certificado

Datos de estado de Revocación

El Servicio de Estado de Revocación (componente KeyOne VA) proporciona información sobre el estado de revocación del certificado a las Partes de Confianza. El servicio de estado de revocación refleja los cambio de estado del certificado, basadas en las peticiones de cambio de estado generadas por el usuario, el CSP o por una tercera parte, y procesadas por el Servicio de Gestión de Revocación.

P_RS.1.1

Los mensajes periódicos que se envían a este servicio son procedentes de Servicios de Gestión de Revocación de confianza.

P_RS.1.2

Los Sistemas Fiables que proporcionan un Servicio de Estado de Revocación en línea DEBEN validar la integridad y autenticidad de los mensajes periódicos recibidos.

Petición/Respuesta del Estado

Una Parte de Confianza que accede a un certificado mediante el Servicio de Directorio, para verificar una firma, requiere chequear el estado de estos certificados. El CSP proporciona un Servicio de Consulta del Estado de Revocación (componente KeyOne VA) con este propósito. El Servicio de consulta del estado de revocación es un servicio online que proporciona el estado de un certificado en tiempo real.

P_RS.2.1

Todas las respuestas sobre el estado del certificado generadas por un Servicio de Consulta de Estado de Revocación online DEBEN estar firmadas electrónicamente por dicho servicio, mediante sus claves de infraestructura.

P_RS.2.2

Los algoritmos/claves de firma utilizados para generar la respuesta sobre el estado SERÁN compatibles con [ALGO].

P_RS.2.4

Los mensajes respuesta DEBEN contener el instante de tiempo en el cuál el Servicio de consulta del Estado de Revocación / emisor firmó la respuesta.

P_RS.3.1

Los siguientes eventos específicos del Servicio de consulta del Estado de Revocación de Certificado DEBEN ser registrados, por un servicio *online*:

- Todas las peticiones y respuestas sobre el estado del certificado.

P.TSS – Servicio de Sellado de Tiempo

Una Autoridad de Sellado de Tiempo (TSA) es una tercera parte de confianza que proporciona servicios de sellado de tiempo, es decir, genera indicadores de tiempo, que pueden usarse como evidencia de que un determinado dato existía antes de un instante en el tiempo (prueba de existencia).

El servicio de sellado de tiempo en esta especificación proporciona únicamente un proceso de sellado de tiempo, que asocia valores de tiempo a datos.

Revisión de la Corrección de la petición

Este componente se diseña para chequear que la petición es correcta y completa. Si el resultado es positivo, los datos se envían como entrada a la Generación de *Time-Stamp Token*.

P_TS1.1

La TSA PUEDE controlar el origen de cada petición antes de chequear su corrección. Una solución para realizar este control podría ser el uso de un mecanismo de autenticidad de origen de los datos.

P_TS1.2

La TSA VERIFICARÁ que la petición de sellado de tiempo utiliza un algoritmo hash especificado de acuerdo a [ALGO].

Generación del Parámetro Tiempo

Este componente usa una fuente de confianza para la distribución de parámetros de tiempo. Estos parámetros serán usados como entrada al proceso de Generación de Sellado de Tiempo.



P_TS2.1

La(s) fuente(s) fiable(s) de la TSA DEBEN estar sincronizadas con *Co-ordinated Universal Time* (UTC) y dentro de las tolerancias que marque la política, por ejemplo, un segundo. Esta fuente puede ser la misma que se requiere para P_SO3.1.

P_TS2.2

El reloj de la TSA se sincronizará con UTC mediante un mecanismo de confianza demostrada.

Generación del *Token* de Sellado de Tiempo

Esta función es la responsable de crear un sello de tiempo que asocie el instante de tiempo actual, un número de serie único, los datos proporcionados para el sellado de tiempo y garantizar los requerimientos de política a la que se adhiere.

P_TS3.1

El Número de Serie usado dentro del TST DEBE ser único para cada TST emitido por una TSA determinada. Esta propiedad DEBE garantizarse incluso después de una interrupción del servicio (ej. caída del sistema).

P_TS3.2

Al igual que se incluye el Parámetro de Tiempo, el TST DEBE incluir la precisión del reloj de tiempo utilizado, si excede del requerido por política de TSA.

P_TS3.3

Se DEBE incluir una indicación de la política bajo la cual fue creado el TST. Los detalles de dicha política están fuera del ámbito de este documento pero PUEDEN indicar las condiciones bajo las cuáles puede usarse el TST, estado de acreditación de la TSA, etc.

Cálculo del *Token* del sello de tiempo

Este componente calcula el *token* del sello de tiempo que se devolverá al cliente. Es el que realmente hace la firma criptográfica de los datos que proporciona la función de generación del *token* de sello de tiempo.

P_TS4.1

Las claves de firma de la TSA DEBEN ser generadas y almacenadas en un módulo criptográfico seguro.

P_TS4.3

Las claves de control de la TSA DEBEN ser almacenadas en un Dispositivo Criptográfico Hardware (HCD).



P_TS4.5

La TSA garantizará que la respuesta TST contiene los mismos datos que se enviaron en la petición.

P_TS4.6

Las claves/algoritmos de firma que utiliza la TSA, CUMPLIRÁN los requerimientos criptográficos especificados en [ALGO], cuando sean de aplicación.

P_TS6.1

Todos los indiciadores de Sellos de Tiempo DEBEN ser archivados de acuerdo a la política P_AR 1.1.

P. SDPS – Servicio de Suministro de Dispositivo de Usuario

Suministro de Dispositivo Criptográfico Seguro (SCDev)

El suministro del dispositivo criptográfico seguro se refiere a la distribución del mismo al subscriptor (una vez preparado).

P_SP2.1

Siempre que sea necesario, el Proveedor de Servicios de Certificación DEBE garantizar, mediante una configuración adecuada del Sistema Fiable, que el Dispositivo es suministrado al supuesto subscriptor y de forma autenticada.

Distribución y creación de los datos de activación

El Dispositivo Criptográfico Seguro y su contenido están protegidos mediante los datos de activación (secretos). El Proveedor de Servicios de Certificación tiene la responsabilidad de generar estos datos de activación iniciales y, posteriormente, distribuirlos de forma segura al subscriptor.

P_SP3.1

El Sistema Fiable DEBE generar los datos de activación iniciales de forma segura.

P_SP3.2

Los Sistemas Fiables DEBEN garantizar que el personal del Proveedor de Servicios de Certificación no puede hacer un uso indebido del mismo en ningún momento.

Esto PUEDE lograrse, ya sea por:

- Procedimientos de seguridad establecidos durante la fabricación y suministro o;
- Proporcionando al subscriptor, los medios necesarios para que PUEDA verificar que la clave privada no ha sido usada antes de la recepción del dispositivo.

CAPÍTULO 4

Objetivos de Seguridad

Esta sección identifica y define los objetivos de seguridad para el Objeto de Evaluación y su entorno. Los objetivos de seguridad reflejan la intención señalada y contrarrestan las amenazas identificadas, al mismo tiempo que cumplen con las políticas de seguridad organizativas y las hipótesis.

Objetivos de Seguridad para el Objeto de Evaluación (TOE)

O1. Integridad de A1,A2,A3, A4, A5, A6, A7.

La integridad de los productos y sistemas del Objeto de Evaluación. Asegura la integridad del usuario y de los datos del TSF que se transfieren internamente dentro del sistema y proporcional la protección de la integridad de los datos personales adecuada. Las funciones de seguridad del Objeto de Evaluación necesitan ser protegidas frente a modificaciones no autorizadas.

O2. Autenticación y Registro de la actividad de los usuarios del Objeto de Evaluación y de cualquier acceso a sus activos

Los usuarios del Objeto de Evaluación necesitan ser identificados, autenticados con mecanismos fuertes y responsables de las acciones relativas a los procesos de certificación y los activos del Objeto de Evaluación. Este registro de la actividad comienza una vez que el usuario ha sido correctamente identificado y autenticado por la aplicación KeyOne, y por lo tanto, pasa a ser considerado un usuario KeyOne que accede a los servicios de certificación proporcionados por las aplicaciones KeyOne.

O3. Confidencialidad de las claves secretas y de la información del usuario

Garantizar la confidencialidad de los procesos de generación de los datos de creación de firma, protegiendo frente a revelación y accesos no autorizado la información clasificada correspondiente, de acuerdo a las normativas de protección de datos. Esto incluye protección frente a revelación y acceso no autorizado a los dispositivos seguros de creación de firma (A4), claves criptográficas (A3), la información de usuario (A1, A2) que se recoge durante el procesos de registro, gestión de certificados o gestión de revocación.

O4. Garantías de las funciones de seguridad del Objeto de Evaluación y de los procesos de desarrollo y operacionales



Garantizar que los cuatro objetivos anteriores se cumplen de forma adecuada por la implementación del Objeto de Evaluación y por la reducción de la probabilidad de vulnerabilidades en los productos del Objeto de Evaluación derivada de la introducción de medidas de seguridad en los procesos de ingeniería del software y durante la vida operativa del sistema, de acuerdo con los estándares y normativas técnicas. Este objetivo pretende principalmente salvaguardar las garantías de seguridad del objeto de evaluación durante la operación del TWS, lo cual conlleva al establecimiento de procedimientos de seguridad operacional.

Objetivos de Seguridad para el Entorno

O5. Disponibilidad de los activos críticos A6, A7, A8, A9 y A10

El sistema del Objeto de Evaluación debe garantizar la oportunidad y disponibilidad de los servicios en tiempo real, como son el registro, la revocación, la validación y el sellado de tiempo, tal y como identifican los requerimientos de política [Cen01c].

Toda la información sobre la actividad del Sistema Fiable debe mantenerse y ser archivada de forma segura, como evidencia legal de la fiabilidad y confianza en la operación del sistema.

O6. Entorno operativo confiable

Los procedimientos y controles del entorno del Objeto de evaluación serán definidos de modo que la operación del mismo se haga conforme a los requerimientos de Política de Seguridad Organizativa establecidos previamente, además de garantizar que los mecanismos de seguridad del Objeto de Evaluación no son evitados con ayuda del entorno.

O7. Integridad de los sistemas de bases de datos y de operación

Se debe proteger la integridad del entorno del sistema que soporta la funcionalidad del Objeto de Evaluación. Garantizar la integridad del usuario y de los datos del TSF transferidos internamente dentro del sistema y proporcionar una adecuada protección de la integridad de los datos de usuario, el software, la información de configuración y de auditoría. Las funciones de seguridad del entorno necesitan protegerse frente a modificaciones no autorizadas.

O8. Responsabilidad y Autenticación de los recursos informáticos del entorno

El acceso lógico y el uso de recursos de las Tecnologías de la Información, debería restringirse mediante la implantación de mecanismos adecuados de identificación, autenticación y autorización, que asocien usuarios y recursos con determinadas reglas de acceso. La información sobre accesos y uso de los recursos del entorno debería quedar registrada, para poder identificar y resolver incidentes relativos a accesos indebidos.

O9. Confidencialidad de los Dispositivos de Seguridad

La confidencialidad requerida para los procesos de generación de los datos de creación de firma usados en certificados de firma QC/NQC y para los mecanismos de autenticación de los oficiales de registro, se extiende también a los procesos de administración y gestión de los dispositivos de seguridad (HSM, SSCD), que se

emplean para la protección de las claves sensibles. Por lo tanto, se necesita una protección adecuada para estos mecanismos del entorno, que prevengan un acceso no autorizado y la revelación de dicha información clasificada.

CAPÍTULO 5

Requisitos de Seguridad de la IT

Requisitos de Seguridad del TOE

Requisitos Funcionales de Seguridad del TOE

The required minimum strength of function level is mandated as "SOF-basic", for the functional requirements indicated in this section. With this SOF, the TOE shall be resistant to attackers with low attack potential, and remaining vulnerabilities shall only be exploitable by attacker with moderate or high attack potential.

FAU – Security audit

Security auditing involves recognizing, recording, storing and analyzing information related to security relevant activities (i.e. activities controlled by the TSP). The resulting audit records can be examined to determine which security relevant activities took place and whom (which user) is responsible for them.

FAU_GEN – Security Audit Data Generation

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

FAU_GEN.1 Audit Data Generation

Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions.

b) All auditable events for the [selection: *no especificada*] level of audit; and

c) [assignment:



- *El éxito y el fallo en la actividad de la aplicación (una vez que la aplicación haya sido arrancada y un usuario de la misma haya sido correctamente identificado y autenticado)*
- *Suministrar un timestamp*
- *Procesar una petición de certificación/revocación*
- *Comenzar/finalizar una sesión de las siguientes aplicaciones: KeyOne CA, KeyOne TSA y KeyOne VA.*
- *Generar una CRL.*
- *Cancelar el procesamiento de un lote.*
- *Todas las peticiones y respuestas relativas al estado de certificados que son recibidas/enviadas por el Servicio de Información de Estado de Revocación*
- *Todos los sellos de tiempo que genera el servicio de Sellado de tiempo]*

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on auditable event definitions of the functional components included in the PP/ST, [assignment: *rol de la identidad del sujeto, nivel del evento (eventos anidados), categoría del evento, observaciones (información adicional relativa al evento), identificador del evento, datos de revocación y datos de certificación*]

FAU_GEN.2 User Identity Association

The TSF shall associate auditable events to individual user identities.

FAU_GEN.2.1

The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR – Security Audit Review

This family defines the requirements for audit tools that should be available to authorized users to assist in the review of audit data.

FAU_SAR.1 Audit Review

This component will provide authorized users the capability to obtain and interpret the information. If human users this information needs to be in human understandable presentation. If external IT entities the information needs to be unambiguously represented in an electronic fashion.

FAU_SAR.1.1

The TSF shall provide [assignment: *usuarios que han sido autenticados por la aplicación KeyOne (administradores de la Autoridad de Certificación, administradores de la Autoridad de Validación y administradores de la Autoridad de Sellado de Tiempo*] with the capability to read [assignment: *toda la información relativa a los registros de auditoría (fecha y hora del evento, tipo del evento, identidad del sujeto, resultado del evento, rol de la identidad del sujeto, nivel del evento, categoría del evento, observaciones e identificador del evento*)] from the audit records.

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit review

Selectable audit review requires audit review tools to select the audit data to be reviewed based on criteria.

FAU_SAR.3.1

The TSF shall provide the ability to perform [selection: *búsquedas, clasificaciones y ordenaciones*] of audit data based on [assignment: *fecha y hora del evento, tipo del evento, identidad del usuario, rol del usuario, identificador del evento, módulo que generó el evento, categoría del evento (importancia del evento), observaciones relativas al evento*].

FAU_STG – Security Audit Event Storage

This family defines the requirements for the TSF to be able to create and maintain a secure audit trail.

FAU_STG.1 Protected Audit Trail Storage

Protected audit trail storage, requirements are placed on the audit trail. It will be protected from unauthorised deletion and/or modification.

FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2_1

The TSF shall be able to [selection: *detectar*] unauthorised modifications to the audit records in the audit trail.

FAU_STG.1.2_2

The TSF shall be able to [selection: *impedir*] unauthorised modifications to the audit records in the audit trail.



FCS – Cryptographic Support

The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel and data separation. This class is used when the TOE implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software.

FCS_CKM – Cryptographic Key Management

Cryptographic keys must be managed throughout their life cycle. This family is intended to support that lifecycle and consequently defines requirements for the following activities: cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction. This family should be included whenever there are functional requirements for the management of cryptographic keys.

FCS_CKM.1 Cryptographic Key Generation

Cryptographic key generation requires cryptographic keys to be generated in accordance with a specified algorithm and key sizes that can be based on an assigned standard.

FCS_CKM.1.1_1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: 3DES] and specified cryptographic key sizes [assignment: 168 bits] that meet the following: [assignment:" FIPS 46-3, Data Encryption Standard (3DES)" junto con una función de generación de números aleatorios de la librería criptográfica OpenSSL (generación de claves y de vectores de inicialización)].

FCS_CKM.1.1_2

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *RSA, DSA*] and specified cryptographic key sizes [assignment: *hasta 4096 bits (RSA), 1024 bits (DSA), y según los requisitos de tamaño especificados en [ALGO]*] that meet the following: [assignment: *RSA Laboratories - PKCS #1 v2.1 - RSA Encryption Standard (RSA), FIPS PUB 186-2 y RFC 3279 (DSA), requisitos criptográficos especificados en [ALGO]*].

FCS_CKM.2 Cryptographic Key Distribution

Cryptographic key distribution requires cryptographic keys to be distributed in accordance with a specified distribution method which can be based on an assigned standard.

FCS_CKM.2.1

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *certificados de clave pública*] that meets the following: [assignment: *X509v3: ITU-T Recommendation X.509 | ISO/IEC International Standard 9594-8, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, política organizativa*



sobre integridad y autenticidad de claves públicas, y cualesquiera parámetros asociados, de acuerdo con [CEN01b] (requisito [KM2.4]), política organizativa sobre las propiedades relativas a los certificados autofirmados de acuerdo con [CEN01b] (requisito [KM2.5])]

FCS_CKM.3 Cryptographic Key Access

Cryptographic key access requires access to cryptographic keys to be performed in accordance with a specified access method which can be based on an assigned standard.

FCS_CKM.3.1

The TSF shall perform [assignment: *todos los accesos a claves criptográficas*] in accordance with a specified cryptographic key access method [assignment: *estándar PKCS #11]* that meets the following: [assignment: *política organizativa sobre la utilización autorizada de claves, de acuerdo con [CEN01b] (requisito [KM3.5]), política organizativa sobre la confianza en certificados de acuerdo con [CEN01b] (requisito [KM3.6]]*.

FCS_COP – Cryptographic Operation

In order for a cryptographic operation to function correctly, the operation must be performed in accordance with a specified algorithm and with a cryptographic key of a specified size. This family should be included whenever there are requirements for cryptographic operations to be performed.

Typical cryptographic operations include data encryption and/or decryption, digital signature generation and/or verification, cryptographic checksum generation for integrity and/or verification of checksum, secure hash (message digest), cryptographic key encryption and/or decryption, and cryptographic key agreement.

FCS_COP.1 Cryptographic Operation

Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

FCS_COP.1.1_1

The TSF shall perform [assignment: *cifrado y descifrado simétrico*] in accordance with a specified cryptographic algorithm [assignment: *DES, 3DES, AES, RC2 y RC4*] and cryptographic key sizes [assignment: *DES (56 bits), 3DES (168 bits), AES (128, 192, 256 bits), RC2 (40, 64, 128 bits), RC4 (128 bits)*] that meet the following [assignment: *FIPS 46-3, Data Encryption Standard (DES/3DES), FIPS PUB 197 (AES), RFC 2268 – A description of the RC2 Encryption Algorithm (RC2)*].

FCS_COP.1.1_2

The TSF shall perform [assignment: *verificación de firmas digitales*] in accordance with a specified cryptographic algorithm [assignment: *RSA con SHA1, RSA con MD2, RSA con MD5, DSA con SHA1*] and cryptographic key sizes [assignment: *RSA (512, 1024, 2048 bits), DSA (512, 1024 bits)*] that meet the following [assignment: *PKCS #1 – RSA Encryption Standard (RSA), FIPS PUB 186-2 (DSA), FIPS PUB 180-1 (SHA1), RFC 1319 – The*



MD2 Message Digest Algorithm (MD2), RFC 1321 – The MD5 Message Digest Algorithm (MD5)].

FCS_COP.1.1_3

The TSF shall perform [assignment: *cifrado asimétrico*] in accordance with a specified cryptographic algorithm [assignment: *combinación de algoritmos de cifrado asimétrico con los algoritmos RSA y DSA*] and cryptographic key sizes [assignment: *RSA (512, 1024, 2048 bits), DSA (512, 1024 bits), DES (56 bits), 3DES (168 bits), AES (128, 192, 256 bits), RC2 (40, 64, 128 bits), RC4 (128 bits)*] that meet the following [assignment: *PKCS #1 – RSA Encryption Standard (RSA), FIPS 46-3, Data Encryption Standard (DES/3DES), FIPS PUB 186-2 (DSA), FIPS PUB 197 (AES), RFC 2268 – A description of the RC2 Encryption Algorithm (RC2)*].

FCS_COP.1.1_4

The TSF shall perform [assignment: *generación y verificación de firmas utilizando criptografía simétrica*] in accordance with a specified cryptographic algorithm [assignment: *3DES con SHA1, algoritmo HMAC*] and cryptographic key sizes [assignment: *3DES (168 bits)*] that meet the following [assignment: *FIPS 46-3, Data Encryption Standard (3DES), FIPS PUB 180-1 (SHA1), RFC 2104 – HMAC: Keyed-Hashing for Message Authentication (HMAC)*].

FCS_COP.1.1_5

The TSF shall perform [assignment: *computación segura de valores resumen*] in accordance with a specified cryptographic algorithm [assignment: *SHA1, MD2 y MD5*] and cryptographic key sizes [assignment: *no aplicable*] that meet the following [assignment: *FIPS PUB 180-1 (SHA1), RFC 1321 – The MD5 Message Digest Algorithm (MD5), RFC 1319 – The MD2 Message Digest Algorithm (MD2), Políticas organizativas P_KM2.5 and P_KM2.6 sobre "huellas dactilares" de certificados autofirmados de acuerdo con [CEN01b]*].

FIA – Identification and Authentication

Identification and Authentication is required to ensure that users are associated with the proper security attributes (e.g. identity, groups, roles, security or integrity levels). The unambiguous identification of authorised users and the correct association of security attributes with users and subjects is critical to the enforcement of the intended security policies. The families in this class deal with determining and verifying the identity of users, determining their authority to interact with the TOE, and with the correct association of security attributes for each authorised user. Other classes of requirements (e.g. User Data Protection, Security Audit) are dependent upon correct identification and authentication of users in order to be effective.

FIA_UID – User Identification

This family defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification.

FIA_UID.1 Timing of Identification

Timing of identification, allows users to perform certain actions before being identified by the TSF.

FIA_UID.1.1

The TSF shall allow [assignment: *cancelar el proceso de identificación*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2 User identification before any action

User identification before any action, require that users identify themselves before any action will be allowed by the TSF.

FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU – User Authentication

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

FIA_UAU.2 User authentication before any action

User authentication before any action, requires that users authenticate themselves before any action will be allowed by the TSF.

FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.6 Re-authenticating

Re-authenticating, requires the ability to specify events for which the user needs to be re-authenticated.

FIA_UAU.6.1

The TSF shall re-authenticate the user under the conditions [assignment: *después del logout*]

FPT – Protection of the TSF

This class contains families of functional requirements that relate to the integrity and management of the mechanisms that provide the TSF (independent of TSP specifics) and to the integrity of TSF data (independent of the specific contents of the TSP data).



In some sense, families in this class may appear to duplicate components in the FDP: User data protection class; they may even be implemented using the same mechanisms. However, FDP: User data protection focuses on user data protection, while FPT: Protection of the TSF focuses on TSF data protection. In fact, components from the FPT: Protection of the TSF class are necessary to provide requirements that the SFPs in the TOE cannot be tampered with or bypassed.

FPT_ITI – Integrity of exported TSF data

This family defines the rules for the protection, from unauthorised modification, of TSF data during transmission between the TSF and a remote trusted IT product. This data could, for example, be TSF critical data such as passwords, keys, audit data, or TSF executable code.

FPT_ITI.1 Inter-TSF detection of modification

Inter-TSF detection of modification, provides the ability to detect modification of TSF data during transmission between the TSF and a remote trusted IT product, under the assumption that the remote trusted IT product is cognisant of the mechanism used.

FPT_ITI.1.1

The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [assignment: *la fuerza de la detección de modificaciones se basa en la fuerza de los algoritmos utilizados en el mecanismo KeyOne i3D y en los algoritmos SHA1 y RSA que están relacionados con el proceso de firma*]

FPT_ITI.1.2

The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [assignment: *generación de un informe*] if modifications are detected.

FPT_ITA – Availability of exported TSF data

This family defines the rules for the prevention of loss of availability of TSF data moving between the TSF and a remote trusted IT product. This data could, for example, be TSF critical data such as password, keys, audit data, or TSF executable code.

FPT_ITA.1 Inter-TSF availability within a defined availability metric

This component requires that the TSF ensure, to an identified degree of probability, the availability of TSF data provided to a remote trusted IT product.

FPT_ITA.1.1

The TSF shall ensure the availability of [assignment: *información de revocación proporcionada por el Servicio de Estado de Revocación*] provided to a remote trusted IT product within [assignment: *el retraso máximo desde la recepción de una petición de revocación y/o suspensión hasta la modificación de la información relativa al estado del certificado no será superior a un día (24 horas)*] given the following conditions [assignment: *no se da una situación de desastre*].

FPT_ITC – Confidentiality of exported TSF data

This family defines the rules for the protection from unauthorised disclosure of TSF data during transmission between the TSF and a remote trusted IT product. This data could, for example, be TSF critical data such as passwords, keys, audit data, or TSF executable code.

FPT_ITC.1 Inter-TSF confidentiality during transmission

This component requires that the TSF ensure that data transmitted between the TSF and a remote trusted IT product is protected from disclosure while in transit.

FPT_ITC.1.1

The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

FDP – User data protection

This class contains families specifying requirements for TOE security functions and TOE security function policies related to protecting user data.FDP: User data protection is split into four groups of families that address user data within a TOE, during import, export, and storage as well as security attributes directly related to user data.

FDP_ITT – Internal TOE transfer

This family provides requirements that address protection of user data when it is transferred between parts of a TOE across an internal channel.

FDP_ITT.1 Basic internal transfer protection

Basic internal transfer protection, requires that user data be protected when transmitted between parts of the TOE.

FDP_ITT.1.1

The TSF shall enforce the [assignment: *SFP de control de acceso incluida en el Apéndice* CPS de KeyOne 2.1] to prevent the [selection: *revelación, modificación*] of user data when it is transmitted between physically-separated parts of the TOE.

FDP_DAU – Data authentication

Data authentication permits and entity to accept responsibility for the authenticity of information (e.g., by digitally signing it). This family provides a method of providing a guarantee of the validity of a specific unit of data that can be subsequently used to verify that the information content has not been forged or fraudulently modified. In contrast to FAU: Security audit, this family is intended to be applied to "static" data rather than data that is being transferred.

FDP_DAU.1 Basic Data Authentication

Basic Data Authentication, requires that the TSF is capable of generating a guarantee of authenticity of the information content of subjects (e.g. documents).



FDP_DAU.1.1

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *la asociación entre los datos de usuario incluidos en la petición de certificación y la clave pública del usuario que solicita la certificación*].

FDP_DAU.1.2

The TSF shall provide [assignment: *Responsable de la Entidad de Certificación*] with the ability to verify evidence of the validity of the indicated information.

FDP_DAU.2 Data Authentication with Identity of Guarantor

Data Authentication with Identity of Guarantor additionally requires that the TSF is capable of establishing the identity of the subject who provided the guarantee of authenticity.

FDP_DAU.2.1

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *la asociación entre los datos de usuario incluidos en la petición de certificación y la clave pública del usuario que solicita la certificación*].

FDP_DAU.2.2

The TSF shall provide [assignment: *Responsable de la Entidad de Certificación*] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

FDP_ACC – Access Control Policy

This family identifies the access control SFPs (by name) and defines the scope of control of the policies that form the identified access control portion of the TSP.

FDP_ACC.1 Subset access control

Subset access control requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE.

FDP_ACC.1.1

The TSF shall enforce the [assignment: *control de acceso basado en los mecanismos de identificación y autenticación*] on [assignment: *recursos de sistema y operaciones ofrecidas por la aplicación*].

Extensión de los requisitos funcionales de seguridad del TOE

Las TSF pueden utilizar funcionalidad criptográfica para ayudar a conseguir varios objetivos de seguridad de alto nivel. Entre ellos se incluyen (pero no se limitan a): identificación y autenticación, no repudio, camino de confianza, canal de confianza y separación de datos. Esta clase se utiliza cuando el TOE implementa funciones

criptográficas, cuya implementación puede estar en hardware, firmware y/o software.

FCS_CKM - Gestión de claves criptográficas

Las claves criptográficas deben ser gestionadas a lo largo de su ciclo de vida. Esta familia está orientada a soportar este ciclo de vida y, en consecuencia, define requisitos para las siguientes actividades: generación de claves criptográficas, distribución de claves criptográficas, acceso a claves criptográficas y destrucción de claves criptográficas. Esta familia debe ser incluida cuando requisitos funcionales relativos a la gestión de claves criptográficas.

FCS_CKM.1 Generación de claves criptográficas

Este componente requiere que las claves criptográficas sean generadas de acuerdo a un algoritmo y a unos tamaños de clave específicos, los cuales pueden estar basados en un estándar asignado. Este componente también establece las condiciones de seguridad bajo las que se generan las claves criptográficas.

FCS_CKM.1.3

Las TSF asegurarán que el modulo criptográfico sólo genere los tipos de claves especificados [asignación: claves de firma *QC/NQC*] cuando se den las siguientes condiciones [asignación: control de dos personas, como mínimo].

FCS_CKM.3 Acceso a las claves criptográficas

Este componente requiere que el acceso a las claves criptográficas se realice según un método de acceso específico, el cual puede estar basado en un estándar asignado, y una protección adecuada de estas claves.

FCS_CKM.3.2

Las TSF deben garantizar que se realizan controles de acceso a todos los módulos criptográficos que utilizan claves de los tipos especificados [asignación: claves de firma *QC/NQC, claves de infraestructura y claves de control*]

FCS_CKP - Protección de claves criptográficas

Las TSF deben establecer requisitos de seguridad para proteger y distribuir de forma segura la clave pública del servicio de generación de certificados QC/NQC, las claves de infraestructura y las claves de control. Debido a la variedad de amenazas que se ciernen sobre las claves de los TWS, que dependen de dónde y cuándo son utilizadas, es importante clasificar las claves de acuerdo a su perfil de riesgo.

FCS_CKP.1 Mecanismos de seguridad aplicados a las claves criptográficas

Este componente requiere la protección de la clave pública del servicio de generación de certificados QC/NQC, de la claves de infraestructura, de las claves control y de las claves de sujeto

FCS_CKP.1.2

Las TSF asegurarán que no existe ninguna función que permita [selección: copia de seguridad, depósito] de los tipos de clave especificados [asignación: *claves de firma de sujeto (claves privadas)*]



FCS_CKP.1.3

Las TSF asegurarán que no existen funciones que permitan el archivado de los tipos de clave especificados [asignación: *claves de firma de sujeto (claves privadas)*].

FCS_CKP.3 Almacenamiento, copia de seguridad y recuperación de claves

Este componente requiere que las TSF garanticen que las funciones para la realización de copias de seguridad de claves y para su recuperación sigan un método específico.

FCS_CKP.3.2

Las TSF deben garantizar que la copia de seguridad, el almacenamiento y la recuperación de claves de los tipos especificados [asignación: *claves privadas de firma NQC/QC, claves de infraestructura, claves de control*] solamente se realizan por [asignación: *personal autorizado*] cuando se dan las siguientes condiciones [asignación: *como mínimo bajo el control de dos personas para claves privadas de firma NQC/QC*].

XCG - Servicio de generación de certificados

La finalidad de esta clase es especificar la gestión de varios aspectos del servicio de generación de certificados. Este servicio crea y firma certificados que se basan en la identidad y demás atributos de un sujeto, según lo verificado por el servicio de registro.

Esta clase proporciona dos familias las cuales soportan los procesos relacionados con la generación de certificados y los requisitos funcionales asociados a la renovación de certificados.

XCG_CGE - Generación de certificados

Esta familia define requisitos de seguridad sobre la generación de certificados. Después de recibir una petición de certificado a través del servicio de registro, los TWSs generan un certificado de la clave pública suministrada. Esto asegura que el CSP blinde el vínculo entre la clave pública del sujeto y la identidad de éste.

Los TWSs también pueden enviar las claves públicas de control y de infraestructura para que sean certificadas por el servicio de generación de certificados. Esto resulta en la producción de certificados de infraestructura y de certificados de control

Después de generar un certificado, éste puede entregarse a través de un dispositivo suplementario de provisión a sujetos o bien puede darse directamente al sujeto.

Los certificados de control y de infraestructura pueden proporcionarse directamente al componente confiable que requiere su uso.

XCG_CGE.1 Procesado de peticiones de certificación

Con este componente, las TSF incorporan requisitos de seguridad sobre el procesamiento de peticiones de certificación.

XCG_CGE.1.1

Las TSF deben asegurar que el servicio de generación de certificados garantiza la [selección: *integridad, autenticidad del origen de los datos, privacidad y confidencialidad*] del mensaje de petición de certificado.

XCG_CGE.1.2

Las TSF deben proporcionar un mecanismo que permita que las peticiones de certificado sean procesadas de forma segura y que se compruebe su conformidad con la política de seguridad aplicable

XCG_CGE.1.3

Las TSFs deben garantizar que antes de la generar un certificado, el TWS se asegure de que la prueba de posesión se realiza satisfactoriamente

XCG_CGE.2 Garantías de los certificados emitidos

Con este componente, las TSF incorporan garantías y propiedades relacionadas con los certificados emitidos.

XCG_CGE.2.1

Las TSF deben garantizar que la clave para firmar certificados cualificados efectivamente sólo se utiliza para firmar dichos certificados y, opcionalmente, para firmar los datos relativos a su estado de revocación

XCG_CGE.2.2

Las TSFs deben garantizar que los certificados emitidos por los TWS tengan las siguientes propiedades [asignación: *indicación del nombre o pseudónimo del sujeto; en el caso de que se utilice un pseudónimo esto deberá indicarse claramente . La clave pública del certificado está relacionada con la clave privada del sujeto. La firma electrónica avanzada del CSP, creada mediante la utilización de las claves de firma del CSP. El certificado debe contener un número de serie distinto y único asignado por el TWS; debe ser único con respecto al CSP emisor. El certificado debe especificar un valor de inicio de su validez que no sea anterior al instante de su emisión y un valor de fin de validez que no preceda al del inicio de validez. Las claves/algoritmos de firma utilizados por el TWS para firmar el certificado deben ser conformes con el estándar [ALGO] sobre especificaciones de algoritmos. El certificado debe incluir una referencia a la política de certificación bajo la cual es emitido*].

XCG_CGE.2.3

Las TSF deben asegurar que los certificados cualificados emitidos por el TWS sean conformes a lo siguiente [asignación: *especificación [TS101862]*].

XCG_CRE - Renovación de certificados

Esta familia define requisitos de seguridad sobre la renovación de certificados. Un certificado pueden renovarse dentro del período previo a su expiración, siendo este período el que defina la política aplicable. La renovación de certificados puede consistir en un escenario de re-emisión de claves: una clave pública nueva se



certifica utilizando información de registro utilizada para generar el certificado previo.

La renovación de certificados abarca los certificados de firma QC/QNC, los certificados de infraestructura, los certificados de control y los certificados de sujeto.

XCG_CRE.1 Renovación de certificados de entidades que no son sujetos

Con este componente las TSF incorporan requisitos de seguridad sobre el proceso de renovación de certificados de firma QC/QNC, de certificados infraestructura y de certificados de control.

XCG_CRE.1.1

Las TSF deben garantizar que las claves de los tipos especificados [asignación: *claves de firma QC/NQC*] se renuevan antes de que expiren y bajo las siguientes condiciones [asignación: *las correspondientes claves públicas renovadas proporcionan al menos el mismo nivel de confianza que cuando fueron inicialmente distribuidas*].

XCG_CRE.2 Renovación de certificados de entidades que son sujetos

Con este componente las TSF incorporan requisitos de seguridad sobre el proceso de renovación de certificados de sujeto.

XCG_CRE.2.1

Las TSF deben garantizar que el mecanismo que se utiliza para [selección, elegir uno de: *regeneración de claves*] de claves de sujeto cumple con las siguientes condiciones [asignación: *debe ser igual de seguro que la generación del certificado inicial*].

FCO - Comunicación

Esta clase proporciona dos familias que se ocupan específicamente de garantizar la identidad del interlocutor que participa en un intercambio de datos. Estas familias están relacionadas con garantizar la identidad del remitente de la información que se transmite (prueba de origen) y con garantizar la identidad del receptor que la recibe (prueba de recepción). Estas familias garantizan que el remitente no pueda negar que haya enviado el mensaje y que el receptor no pueda negar que lo ha recibido

FCO_POM - Protección de mensajes

Esta familia define las reglas para detectar la modificación de datos de TSF durante su transmisión y protege a los datos de TSF del desvelo no autorizado

Esa familia consta sólo del componente FCO_POM.1, protección de los mensajes creados por los servicios fundamentales, que requiere que las TSF sean capaces de evitar los ataques de repetición y que las TSF proporciones marcas de tiempo fiables a las funciones TSF

FCO_POM.1 Protección de los mensajes que son creados por los servicios fundamentales

Con este componente, las TSF incorporan restricciones sobre la protección de datos de TSF durante su transmisión entre componentes distintos de las TSF.

FCO_POM.1.1

Las TSF deben garantizar que los mensajes especificados, creados por los servicios fundamentales [asignación: *mensajes intercambiados en la comunicación entre los componentes KeyOne VA y KeyOne CA, y mensajes intercambiados en la comunicación entre los componentes KeyOne CA y KeyOne LRA]* se protegen utilizando las claves de infraestructura, contienen la hora del mensaje para indicar el momento en el cual el emisor creó el mensaje, e incluyen protección frente a los ataques de repetición.

XR - Servicio de Registro

Esta clase proporciona dos familias que proporcionan los requisitos de seguridad que necesita un servicio de registro. El servicio de registro verifica la identidad y, si procede, cualesquiera atributos específicos de un sujeto. Los resultados de este servicio se pasan al servicio de generación de certificados. Las familias que se incluyen en esta clase soportan la disponibilidad de los mecanismos de seguridad requeridos, tales como la protección de las peticiones de certificación o la protección de los datos del sujeto.

XR_CAP - Solicitud de certificados

Esta familia define requisitos de seguridad sobre la solicitud de certificados, como los mecanismos de protección que se utilizan en las peticiones de certificación, o la colección de datos obtenidos por esta solicitud de certificación.

Un oficial de registro, verifica con los medios apropiados, de conformidad con las leyes nacionales, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se emite un NQC/QC

XR_CAP.1 Protección de las peticiones de certificación

Con este componente las TSF incorporan restricciones sobre la protección de las peticiones de certificación

XR_CAP.1.1

Las TSF deben garantizar que las peticiones de certificación sean protegidas antes de ser enviadas desde el servicio de registro al servicio de generación de certificados, garantizándose así [selección: *confidencialidad del mensaje, autenticación, integridad de datos]*, mediante la utilización de los tipos de claves especificados [asignación: *claves de infraestructura y claves de control*]

XR_CAP.1.2

Las TSF deben proporcionar un mecanismo que permite la aprobación de peticiones de certificación por [asignación: *un oficial de registro*] antes de que abandonen el servicio de registro



XR_CAP.2 Colección de datos de usuario

Con este componente las TSF incorporan los requisitos concernientes a los datos que deben estar contenidos en las peticiones de certificación.

XR_CAP.2.1

Las TSF deben garantizar que el sistema de registro se configurado de forma que permita la obtención de datos de usuario que sean suficientes para satisfacer los requisitos sobre certificados cualificados, de acuerdo con lo siguiente [asignación: *tal y como se especifica en el Anexo 1 de [Eur99a]*]

XRM - Servicio de gestión de la revocación de certificados

La finalidad de esta clase es especificar la gestión de varios aspectos del servicio de gestión de la revocación y del servicio de estado de revocación.

El servicio de gestión de la revocación se encarga de procesar las peticiones y los reportes relativos a la revocación para determinar las acciones necesarias que deben llevarse a cabo. Los resultados de este servicio se distribuyen mediante el servicio de estado de revocación.

El servicio de estado de revocación proporciona información de estado de revocación a interlocutores dependientes. Este servicio puede ser un servicio en tiempo real o puede estar basado en información de estado de revocación que se actualiza a intervalos regulares.

Esta clase proporciona dos familias que soportan el proceso relacionado con las peticiones de cambio de estado de certificados, y los procesos relacionados con la revocación/suspensión de certificados.

XRM_CSC - Peticiones de cambio de estado de certificados

Esta familia define requisitos de seguridad sobre las peticiones de cambio de estado de certificados. Cuando un sujeto sospecha que su clave privada puede haber sido comprometida, debe enviar a los TWS de su CSP una petición de suspensión (revocación temporal) de su certificado. El sujeto también podrá realizar la correspondiente petición para reestablecer la operatividad del certificado.

Cuando el sujeto conoce que su clave privada ha sido efectivamente comprometida, envía una petición de revocación de su certificado a los TWS de su CSP.

El CSP también puede solicitar cambios de estado de certificados a través de este servicio. El estado de los certificados de control y de los certificados de infraestructura se puede controlar también a través de este servicio. Las peticiones para cambiar el estado de un certificado son mensajes autenticados que pueden ser aceptados o rechazados por el CSP.

XRM_CSC.1 Requisitos de seguridad sobre peticiones de revocación

Con este componente, las TSF incorporan requisitos de seguridad sobre el procesamiento de peticiones de cambio de estado de certificados.

XRM_CSC.1.1

Las TSF deben garantizar que no puedan restablecerse los certificados que haya sido definitivamente revocados.

XRM_CSC.1.2

Las TSF deben garantizar que las peticiones de suspensión, restablecimiento y revocación sean convenientemente procesados cuando se den las siguientes condiciones de seguridad [selección: *autenticación, validación]*.

XRM_CSC.1.3

Las TSF deben garantizar que la revocación de certificados que correspondan a claves de firma de QC/QNC sólo sea posible bajo las siguientes condiciones [asignación: *bajo el control de dos personas, como mínimo*].

XRM_CSC.2 Suspensión/Revocación de certificados

Este componente establece acciones que realizar después que se haya completado el procesamiento de una petición/reporte.

XRM_CSC.2.1

El TSF debe garantizar que la base de datos de estados de certificado sea actualizada [asignación: *inmediatamente]* después de que el procesamiento de la petición/reporte se haya completado.

XRM_CSR - Suspensión/Revocación de certificados

Esta familia establece requisitos de seguridad sobre la suspensión/revocación de certificados. El TWS que reciba una petición de suspensión o revocación a través de este servicio, cambia el estado del certificado, bien sea a suspendido o bien a revocado, en su base de datos de estados de certificado, y esto a su vez es utilizado por el servicio de estado de revocación del CSP.

XRM_CSR.1 Proceso de actualización del servicio de estado de revocación

Con este componente, las TSF incorporan requisitos de seguridad sobre el proceso de actualización desde el sistema de gestión de la revocación hacia el servicio de estado de revocación.

XRM_CSR.1.1

Las TSF deben garantizar que cuando se utilice el envío periódico de mensajes, el TWS cumpla los siguientes requisitos

- Para un repositorio de estado *offline* (e.g CRL accesible mediante directorios) el servicio de estado de revocación es actualizado al menos diariamente.
- Para un repositorio de estado *online* (e.g servidor OCSP) el servicio de estado de revocación se actualiza cuando ocurre un cambio de estado y, adicionalmente, al menos diariamente.
- Cada mensaje de actualización incluye el nombre y la firma digital del emisor del mensaje, y la hora del cambio de estado.



- Los mensajes indican que certificados están revocados/suspendidos
- Para cada certificado de la lista, su número de serie y la razón del cambio de su estado son incluidas dentro del mensaje.

XRS - Servicio de estado de revocación de certificados

Esta clase proporciona dos familias, las cuales contienen los requisitos de seguridad sobre el servicio de estado de revocación de certificados.

El servicio de estado de revocación proporciona información sobre el estado de revocación de certificados a los interlocutores dependientes. Este servicio puede ser un servicio en tiempo real o puede estar basado en información de estado de revocación que se actualiza a intervalos regulares. El servicio de estado de revocación debe obtener información fiable de la base de datos de estados de certificado, en la que los procesos de gestión de la revocación insertan la información de estados de certificado.

Las familias incluidas en esta clase soportan la disponibilidad de mecanismos de seguridad necesarios como la protección de las peticiones y respuestas de estado, o la protección de la comunicación entre el proceso de gestión de la revocación y el servicio de estado de revocación.

El servicio de estado de revocación puede ser un servicio *online* (que proporciona el estado del certificado en tiempo real) o un servicio *offline* (en el que el estado del certificado no es en tiempo real)

Donde sea un servicio *online* un interlocutor dependiente, se comunicará con el servicio de estado de revocación y éste le proporcionará los detalles del o de los certificados cuyo estado pregunte. El servicio de estado de revocación *online*, cuando utilice un sistema de envío de mensajes en tiempo real, realizará una consulta a la base de datos de estados de certificado para obtener el estado actual del certificado que se solicite o, si utiliza el envío periódico de mensajes, consultará sus registros internos, los cuales habrán sido actualizados por el último mensaje periódico. De este modo se crea una respuesta y se envía al interlocutor dependiente indicando el estado del o de los certificados solicitados. Donde sea un servicio *offline* el servio de estado de revocación mantendrá el mensaje periódico más reciente. Éste podría ser obtenido por el interlocutor dependiente para comprobar el estado de un certificado.

XRS_RSD - Datos de estado de revocación

Esta familia define requisitos de seguridad sobre la comunicación entre el servicio de estado de revocación y el servicio de gestión de revocación. Esta comunicación consiste en la transferencia de información de estado de certificados desde la base de datos de estados de certificado al servicio de estado de revocación.

El servicio de estado de revocación proporciona información sobre el estado de revocación de certificados a los interlocutores dependientes. El servicio de estado de revocación refleja los cambios de estado de certificado producidos a partir de peticiones de cambio procedentes tanto del titular, como del CSP , como de un tercero y que han sido procesadas por el servicio de gestión de la revocación. Estos datos también pueden ponerse a disposición de los titulares de certificados si la política requiere que los titulares tengan acceso a los datos de estado de revocación.



XRS_RSD.1 Confianza del servicio de estado de revocación

Con este componente se incorporan restricciones sobre la confianza del servicio de estado de revocación.

XRS_RSD.1.1

Las TSF deben garantizar que [selección: *los mensajes periódicos*] proporcionados al servicio de estado de revocación proceden únicamente de servicios de gestión de la revocación que son de confianza.

XRS_RSD.2 Comunicación entre la base de datos de estados de certificado y el servicio de estado de revocación

Con este componente, las TSF incorporan los requisitos concernientes a la seguridad que se aplica a las comunicaciones entre el servicio de estado de revocación y el servicio de gestión de la revocación.

XRS_RSD.2.1

Las TSF deben garantizar que los TWSs que proporcionan un servicio de revocación en línea validan la [selección: *integridad, autenticidad*] de los [selección: *mensajes periódicos*] que se le envían

XRS_SRR - Peticiones/Respuestas de estado

Esta familia define requisitos de seguridad que son necesarios para proteger las peticiones/respuestas entre un interlocutor dependiente y el servicio de estado de revocación

Un interlocutor dependiente que haya obtenido el o los certificados necesarios para la verificación de una firma, necesita comprobar el estado de dichos certificados. El CSP proporciona un servicio de estado de estado de revocación para este propósito

Los TWS pueden exigir que los interlocutores dependientes firmen digitalmente las peticiones de información sobre el estado de certificados. Los TWS pueden opcionalmente proporcionar integridad y confidencialidad a la sesión. Las peticiones de información de estado pueden ser generadas por los propios TWS para obtener el estado de los certificados de firma de NQC/QC, de los certificados de infraestructura y de los certificados de control.

XRS_SRR.1 Protección de las peticiones/respuestas de estado

Con este componente, las TSF incorporan los requisitos necesarios para proteger el protocolo entre el interlocutor dependiente y el servicio de estado de revocación.

XRS_SRR.1.1

Las TSF deben garantizar que el servicio de estado de revocación firma digitalmente todas las respuestas de estados de certificado que genera, utilizando [selección: *acorde con [ALGO]*].

XRS_SRR.1.2

Las TSF deben garantizar que el mensaje de respuesta contenga la hora en la que el emisor del servicio de estado de revocación firmó la respuesta.



XTS - Servicio de sellado de tiempo

Esta clase proporciona dos familias que soportan los mecanismos de seguridad necesarios para el servicio de sellado de tiempo.

Una autoridad de sellado de tiempo (TSA) es una tercera parte de confianza que proporciona un servicio de sellado de tiempo, i.e de generación de sellos de tiempo, los cuales pueden servir como prueba de que ciertos datos existían con anterioridad a un determinado instante de tiempo(prueba de existencia).

Un servicio de sellado de tiempo proporciona un proceso de sellado de tiempo, el cual vincula criptográficamente instantes de tiempo a datos

XTS_REG - Generación de respuestas de sellado de tiempo

Esta familia define los requisitos de seguridad necesarios para generar respuestas de sellado de tiempo.

Esta familia define funciones para los siguientes propósitos:

- Generación de parámetros de tiempo. Estas funciones utilizan una fuente fiable para entregar parámetros de tiempo que sean precisos. Estos parámetros se utilizan como entrada del proceso de generación de sellos de tiempo.
- Generación de sellos de tiempo. Estas funciones son responsables de la creación de un sello de tiempo que vincula la hora vigente, un número de serie único y los datos proporcionados para el sellado, asegurando que se observan todos los requisitos de la política.
- Computación del sellado de tiempo. Estas funciones computan el sello de tiempo que se devuelve al cliente. Estas funciones firman criptográficamente los datos proporcionados por la función de generación de sellos de tiempo.

XTS_REG.2 Contenido de las respuestas de sellado de tiempo

Con este componente, las TSF incorporan los requisitos necesarios para incluir datos en el contenido de una respuesta de sellado de tiempo.

XTS_REG.2.1

Las TSF deben garantizar que el número de serie que se utiliza dentro del TST sea único entre los TST emitidos por una TSA dada. Esta propiedad debe cumplirse cuando ocurren las siguientes condiciones [asignación: *siempre, incluso después de una posible interrupción (e.g caída del servicio)*].

XTS_REG.2.3

Las TSF deben garantizar que se incluya una indicación de la política bajo la cual se haya creado el TST.

XTS_REG.2.4

Las TSF deben garantizar que la respuesta TST contenga los mismos datos que fueron enviados en la petición.

XTS_REG.3 Garantías de seguridad de las respuestas de sellado de tiempo

Con este componente, las TSF incorporan los requisitos necesarios para garantizar la seguridad de las respuestas de sellado de tiempo que se generan.

XTS_REG.3.1

Las TSF deben garantizar que los algoritmos/claves de firma que utiliza la TSA satisfacen lo siguiente [asignación: *requisitos criptográficos especificados en [ALGO]*].

XSP - Servicio de entrega de dispositivos a sujetos

La finalidad de esta clase es especificar la gestión de varios aspectos del servicio de entrega de dispositivos a sujetos.

El servicio de entrega de dispositivos a los sujetos, prepara y proporciona dispositivos de creación de firma a los sujetos. Ejemplos de este servicio son:

- Un servicio que genera los pares de claves de los sujetos y les proporciona la claves privadas.
- Un servicio que prepara los dispositivos de creación de firma segura de los sujetos (SSCD) y los códigos activadores de dichos dispositivos y los entrega a los sujetos registrados.

Este servicio puede proporcionar un SCDev y/o un SSCD. Los requisitos de seguridad aplicables a los SCDs también son aplicables a los SSCDs, donde los SSCDs cumplen los requisitos adicionales que se establecen en el Anexo III de [Eur99a]. No se hace ninguna distinción respecto a si el SCDev/SSCD se implementa en hardware o en software.

XSP_SDP - Entrega de SCDev

Esta familia define los requisitos de seguridad aplicables a la distribución de SCDev (después de su preparación) a los sujetos.

XSP_SDP.1 Distribución de SCDev

Con este componente, las TSF incorporan requisitos de seguridad sobre el proceso de distribución de los SCDev a los sujetos.

XSP_SDP.1.1

Las TSF deben garantizar mediante la configuración adecuada del TWS que los SCDev se entregan a los sujetos autenticados a los que les corresponde.

XSP_ACD - Creación y distribución de los datos de activación

Esta familia define los requisitos de seguridad aplicables a la creación y distribución de los datos de activación. Los SCDev y su contenido están protegidos con datos secretos de activación. El CSP es responsable de la generación de estos datos de activación y de su posterior distribución segura a los sujetos.



XSP_ACD.1 Garantías de la creación y distribución de datos de activación

Con este componente, las TSF incorporan requisitos de seguridad sobre los procesos de creación y distribución de datos de activación.

XSP_ACD.1.1

Las TSF deben garantizar que el [asignación: *personal del CSP*] nunca pueda hacer un mal uso de los SCDev.

Requisitos de Aseguramiento de Seguridad del TOE

Los componentes de aseguramiento seleccionados son aquellos especificados para cumplir con el nivel de aseguramiento EAL2, tal y como se indica en la siguiente tabla:

Clase de Aseguramiento	Componente de Aseguramiento
Gestión de Configuración	ACM_CAP.2
Entrega y Operación	ADO_DEL.1, ADO_IGS.1
Desarrollo	ADV_FSP.1, ADV_HLD.1, ADV_RCR.1
Documentos de Guía	AGD_ADM.1, AGD_USR.1
Pruebas	ATE_COV.1, ATE_FUN.1, ATE_IND.2
Análisis de Vulnerabilidades	AVA_SOF.1, AVA_VLA.1

ACM – Gestión de Configuración

ACM_CAP – Capacidades de la CM

Las capacidades del sistema CM están orientadas a la gestión de las modificaciones accidentales o no autorizados de los elementos de configuración. El sistema CM debería asegurar la integridad del TOE desde las etapas iniciales de diseño y a través de todas las tareas de mantenimiento siguientes.

ACM_CAP.2 Elemento de Configuración

Se requiere una única referencia para asegurar que no hay ambiguedad en términos de qué instancia del TOE se está evaluando. El etiquetado del TOE con su referencia asegura que los usuarios del TOE tienen conciencia de qué instancia del TOE están utilizando.

Una única identificación de los elementos de configuración conduce a una comprensión más clara de la composición del TOE, lo cual además ayuda a determinar qué elementos están sujetos a los requisitos de evaluación para el TOE.

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labelled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7C The CM system shall uniquely identify all configuration items.

ADO – Entrega y Operación

Entrega y operación provee requisitos para gestionar de manera adecuada los procesos de entrega, instalación, generación y puesta en marcha del TOE.

ADO_DEL - Entrega

Los requisitos para la entrega requieren facilidades de control y distribución del sistema y procedimientos que provean aseguramiento de que los receptores reciben el TOE que el emisor intentó enviar, sin ninguna modificación. Para una entrega correcta, lo que se recibe debe corresponderse de manera precisasa con una copia maestra del TOE, y de este modo evitar cualquier falsificación en la versión real, o sustitución con una versión falsa.

ADO_DEL.1 Procedimientos de Entrega

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_IGS - Instalación, generación y puesta en marcha

Los procedimientos de instalación, generación y puesta en marcha son útiles para asegurar que el TOE ha sido instalado, generado y se ha puesto en marcha de una manera segura tal y como pretende el desarrollador. Los requisitos para la instalación, generación y puesta en marcha requieren una transición segura desde la representación de la implementación del TOE que se encuentra bajo control de configuración, hasta su operación inicial en el entorno del usuario.

ADO_IGS.1 Procedimientos de instalación, generación y puesta en marcha

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.



ADV – Desarrollo

La Clase Desarrollo abarca cuatro familias de requisitos que representan el TSF en varios niveles de abstracción desde la interfaz funcional a la representación de la implementación. La Clase Desarrollo también incluye una familia de requisitos que realiza una correspondencia entre las varias representaciones del TSF, requiriendo también una demostración de la correspondencia desde la presentación menos abstracta a través de todas las representaciones que intervienen en la especificación del sumario del TOE provista en la Declaración de Seguridad. Adicionalmente hay una familia de requisitos para un modelo del TSP, y para la correspondencia entre el TSP, el modelo del TSP, y la especificación funcional. Finalmente, hay una familia de requisitos basada en la estructura internal del TSF, la cual cubre aspectos tales como la modularidad, el diseño, y la minimización de la complejidad.

ADV_FSP – Especificación funcional

La especificación funcional es una descripción de alto nivel de las interfaces visibles por el usuario y el comportamiento del TSF. Hay una instanciación de los requisitos funcionales de seguridad del TOE. La especificación funcional tiene que mostrar cómo se cubren todos los requisitos funcionales de seguridad del TOE.

ADV_FSP.1 Especificación funcional informal

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

ADV_HLD – Diseño de alto nivel

El diseño de alto nivel de un TOE provee una descripción del TSF en términos de unidades estructurales mayores (por ejemplo subsistemas) y relaciona estas unidades con las funciones que éstas proveen. Los requisitos del diseño de alto nivel están orientados a proveer aseguramiento de que el TOE provee una arquitectura apropiada para implementar los requisitos funcionales de seguridad del TOE.

El diseño de alto nivel refina la especificació funcional es subsistemas. Para cada subsistema del TSF, el diseño de alto nivel describe su propósito y función, e identifica las funciones de seguridad incluidas en el subsistema. Las interrelaciones de todos los subsistemas están también definidas en el diseño de alto nivel. Estas interrelaciones se representarán como interfaces externas para el flujo de datos, flujo de control, etc.

ADV_HLD.1 Diseño de alto nivel descriptivo

ADV_HLD.1.1C The presentation of the high-level design shall be informal.



ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/ or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_RCR – Representación de la correspondencia

La correspondencia entre las varias representaciones del TSF (como por ejemplo la especificación del sumario del TOE, especificación funcional, diseño de alto nivel, diseño de bajo nivel, representación de la implementación) dirige la instanciación completa y correcta de los requisitos a la representación más abstracta del TSF provista. Esta conclusión se consigue mediante el refinamiento paso a paso y los resultados acumulativos de las determinaciones de correspondencia entre las abstracciones adyacentes de representaciones.

ADV_RCR.1 Demostración de correspondencia informal

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

AGD – Documentos de Guía

La Clase sobre documentos de guía provee los requisitos para la documentación de guía del usuario y administrador. Para la administración segura y uso del TOE es necesario describir todos los aspectos relevantes para una aplicación segura del TOE.

AGD_ADM – Guía de Administrador

La guía de Administrador se refiere a material escrito que está orientado a ser usado por aquellas personas responsables de configurar, mantener y administrar el TOE de una manera correcta para alcanzar la seguridad máxima. Puesto que la operación segura del TOE es dependiente del correcto funcionamiento del TOE, las personas responsables de ejecutar estas funciones son personas de confianza por el TSF. La guía del administrador está orientada a ayudar a los administradores a entener las



funciones de seguridad provistas por el TOE, incluyendo tanto las funciones que requieren el administrador para ejecutar acciones criticas de seguridad, como aquellas funciones que proveen información crítica de seguridad.

AGD_ADM.1 Guía del Administrador

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_USR – Guía del Usuario

La guía del usuario se refiere al material que está orientado a ser usado por usuarios humanos no administradores del TOE, y por otros tipos de personal (por ejemplo programadores) que usan las interfaces externas del TOE. La guía del usuario describe las funciones de seguridad provistas por el TSF y provee instrucciones y guías, incluyendo avisos, para su uso seguro.

AGD_USR.1 Guía del Usuario

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.



AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

ATE - Pruebas

La clase "Pruebas" está compuesta por cuatro familias: cubrimiento (ATE_COV), profundidad (ATE_DPT), pruebas independientes (por ejemplo pruebas funcionales ejecutadas por evaluadores) (ATE_IND), y pruebas funcionales (ATE_FUN). Las pruebas ayudan a demostrar que los requisitos funcionales de seguridad del TOE se cumplen. Las pruebas proveen aseguramiento de que el TOE satisface como mínimo los requisitos funcionales de seguridad del TOE, aunque no pueda ser establecido que el TOE no hace más de lo que se ha especificado. Las pruebas también pueden ser dirijidas hacia la estructura interna del TOE, como por ejemplo las pruebas de los subsistemas y módulos contra sus especificaciones.

ATE_COV - Cubrimiento

Esta familia está dirigida a aquellos aspectos de las pruebas que tratan sobre la plenitud del cubrimiento de los test. Esta gestiona el alcance de las pruebas del TSF, y si las pruebas son o no suficientemente extensas para demostrar que el TSF opera tal y como se ha especificado.

ATE_COV.1 Evidencia de cubrimiento

En este componente el objetivo es establecer que el TSF ha sido probado contro su especificación funcional. Esto se puede llevar a cabo mediante un examen de la evidencia del desarrollador de la correspondencia.

Mientras el objetivo de las pruebas es cubrir el TSF, no hay ningún requisito para verificar esta declaración, salvo una correspondencia informal de las pruebas a la especificación funcional y los propios datos de las pruebas.

En este componente se requiere del desarrollador que muestre cómo las pruebas que han sido identificadas se corresponden con el TSF tal y como se describe en la especificación funcional. Esto se puede conseguir mediante una declaración de correspondencia, posiblemente utilizando una tabla. Esta información se requiere para apoyar al evaluador en la planificación del programa de las pruebas para la evaluación. En este nivel no hay requisitos para un cubrimiento completo por parte del desarrollador de cada aspecto del TSF, y el evaluador necesaritará tener en cuenta cualquier deficiencia en este área.

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.1.1D The developer shall provide evidence of the test coverage.



ATE_FUN – Pruebas Funcionales

Las pruebas funcionales ejecutadas por el desarrollador establecen que el TSF muestra las propiedades necesarias para satisfacer los requisitos funcionales de su PP/ST. Tales pruebas funcionales proveen aseguramiento de que el TSF satisface como mínimo los requisitos funcionales de seguridad, aunque no puedan establecer que el TSF no hace nada más de lo que se ha especificado.

La familia "Pruebas Funcionales" está centrada en el tipo y cantidad de documentación o herramientas de soporte requeridas, y lo que se tiene que demostrar a través de las pruebas del desarrollador. Las pruebas funcionales no están limitadas a una confirmación positiva de que las funciones de seguridad requeridas se satisfacen, sino que pueden incluir también pruebas negativas para comprobar la ausencia de un comportamiento particular no deseado (a menudo basado en la inversión de requisitos funcionales).

ATE_FUN.1 Pruebas funcionales

El objetivo es que el desarrollador demuestre que todas las funciones de seguridad se ejecutan tal y como se especificaron. Se requiere que el desarrollador ejecute pruebas y provea documentación de pruebas.

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function.

These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_IND – Pruebas independientes

Un objetivo es demostrar que las funciones de seguridad se ejecutan tal y como fueron especificadas. Un objetivo adicional es mostrar el riesgo de una evaluación incorrecta de los resultados de las pruebas por parte del desarrollador que resulta en una implementación incorrecta de las especificacines, o descuidar código que no cumple las especificaciones.

ATE_IND.2 Pruebas independientes - muestra

El objetivo es demostrar que las funciones de seguridad se ejecutan tal y como se han especificado. Las pruebas del evaluador incluyen una selección y repetición de una muestra de las pruebas del desarrollador. El objetivo es que el desarrollador



debiera proveer al evaluador el material necesario para una reproducción eficiente de las pruebas del desarrollador. Esto puede incluir tales cosas como documentación de pruebas legible por la máquina, programas de pruebas, etc.

Este componente contiene un requisito que exige que el evaluador tenga disponible los resultados de las pruebas del desarrollador, para completar el programa de pruebas. El evaluador repetirá una muestra de pruebas del desarrollador para tener garantías de los resultados obtenidos. Habiendo establecido tal garantía el evaluador se basará en las pruebas del desarrollador realizando pruebas adicionales que hagan funcionar el TOE de una manera diferente. Utilizando una plataforma de resultados de pruebas validadas del desarrollador, el evaluador es capaz de obtener garantías de que el TOE opera correctamente en una más amplia variedad de condiciones que sería posible puramente utilizando los esfuerzos del propio desarrollador, dando un nivel fijo de recursos. Habiendo tenido la seguridad de que el desarrollador ha probado el TOE, el evaluador tendrá también más autonomía, cuando sea apropiado, para concentrar las pruebas en áreas donde el examen de documentación o el conocimiento del especialista ha levantado inquietudes particulares.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developers functional testing of the TSF.

AVA – Análisis de Vulnerabilidad

La clase se basa en la existencia de canales secretos explotables, la posibilidad de hacer un mal uso o de que exista una configuración incorrecta del TOE, la posibilidad de romper mecanismos probabilísticos o permutacionales, y la posibilidad de vulnerabilidades explotables introducidas en el desarrollo o la explotación del TOE.

AVA_SOF – Fortaleza de las funciones de seguridad del TOE

Incluso si una función de seguridad del TOE no puede ser circunvalada, desactivada, o corrompida, puede ser posible aún así vencida porque existe una vulnerabilidad en el concepto de sus mecanismos de seguridad subyacentes. Para estas funciones se puede hacer una calificación de su comportamiento de seguridad usando los resultados de un análisis cuantitativo o estadístico del comportamiento de seguridad de estos mecanismos y el esfuerzo requerido para vencerlas. La calificación se hace en la forma de fortaleza de la función de seguridad del TOE.

AVA_SOF.1 Fortaleza de la evaluación de las funciones de seguridad del TOE

Las funciones de seguridad se implementan mediante mecanismos de seguridad. Por ejemplo, un mecanismo de contraseña puede usarse en la implementación de la función de seguridad de identificación y autenticación.

La fortaleza de la evaluación de la función de seguridad del TOE se lleva a cabo en el nivel del mecanismo de seguridad, pero sus resultados proveen conocimiento sobre la habilidad de la función de seguridad referida para resistirse a las amenazas identificadas. La fortaleza del análisis de las funciones de seguridad del TOE deberían



considerar como mínimo los contenidos de todos los deliverables del TOE, incluyendo el ST, para el nivel de seguridad de evaluación necesario.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_VLA – Análisis de Vulnerabilidad

El análisis de vulnerabilidad es una evaluación para determinar si las vulnerabilidades identificadas, durante la evaluación de la construcción y operación anticipada del TOE, o por otros métodos (por ejemplo por hipótesis defectuosas), podrían permitir a los usuarios violar el TSP.

AVA_VLA.1 Análisis de vulnerabilidad del desarrollador

El desarrollador realiza un análisis de vulnerabilidad para determinar la presencia de vulnerabilidades de seguridad obvias, y confirmar que éstas no pueden ser explotadas en el entorno de desarrollo del TOE. El evaluador debería considerar la ejecución de pruebas adicionales como un resultado de vulnerabilidades explotables potenciales identificadas durante otras partes de la evaluación.

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Requisitos de Seguridad para el entorno del IT

This section identifies the IT security requirements that are to be met by the IT environment of the TOE.

FCS – Soporte Criptográfico

The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel and data separation. This class is used when the TOE implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software.

FCS_CKM – Cryptographic Key Management

Cryptographic keys must be managed throughout their life cycle. This family is intended to support that lifecycle and consequently defines requirements for the following activities: cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction. This family should be included whenever there are functional requirements for the management of cryptographic keys.

FCS_CKM.1 Cryptographic Key Generation

Cryptographic key generation requires cryptographic keys to be generated in accordance with a specified algorithm and key sizes that can be based on an assigned standard.

FCS_CKM.1.1_2

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *RSA, DSA*] and specified cryptographic key sizes [assignment: *hasta 4096 bits (RSA), 1024 bits (DSA), y de acuerdo a los requisitos de tamaño especificados en [ALGO]*] that meet the following: [assignment: *RSA Laboratories - PKCS #1 v2.1 - RSA Encryption Standard (RSA), FIPS PUB 186-2 y RFC 3279 (DSA), requisitos criptográficos especificados en [ALGO]*].

FCS_CKM.2 Cryptographic Key Distribution

Cryptographic key distribution requires cryptographic keys to be distributed in accordance with a specified distribution method which can be based on an assigned standard.

FCS_CKM.2.1

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *certificados de clave pública, Directorio, mecanismos offline*] that meets the following: [assignment: *X509v3: ITU-T Recommendation X.509 | ISO/IEC International Standard 9594-8, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, LDAPv2: RFC 1777 – Lightweight Directory Access Protocol, ninguno, política organizativa sobre integridad y autenticidad de las claves públicas y sus parámetros asociados, de acuerdo con [CEN01b] (requisito [KM2.4], política organizativa concerniente a las propiedades relativas a los certificados autofirmados de acuerdo con [CEN01b] (requisito [KM2.5])*]



FCS_CKM.4 Cryptographic Key Destruction

Cryptographic key destruction requires cryptographic keys to be destroyed in accordance with a specified destruction method which can be based on an assigned standard.

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cualquier método FIPS para la destrucción de claves*] that meets the following: [assignment: *FIPS 140-2 nivel 3 o estándares ITSEC E4*].

FCS_COP – Cryptographic Operation

In order for a cryptographic operation to function correctly, the operation must be performed in accordance with a specified algorithm and with a cryptographic key of a specified size. This family should be included whenever there are requirements for cryptographic operations to be performed.

Typical cryptographic operations include data encryption and/or decryption, digital signature generation and/or verification, cryptographic checksum generation for integrity and/or verification of checksum, secure hash (message digest), cryptographic key encryption and/or decryption, and cryptographic key agreement.

FCS_COP.1 Cryptographic Operation

Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

FCS_COP.1.1_6

The TSF shall perform [assignment: *generación aleatoria de semillas*] in accordance with a specified cryptographic algorithm [assignment: *algoritmo propietario utilizado por la librería criptográfica*] and cryptographic key sizes [assignment: *no aplicable*] that meet the following [assignment: *algoritmo propietario de OpenSSL*].

FCS_COP.1.1_7

The TSF shall perform [assignment: *generación de firmas digitales*] in accordance with a specified cryptographic algorithm [assignment: *RSA con SHA1, RSA con MD2, RSA con MD5, DSA con SHA1*] and cryptographic key sizes [assignment: RSA (512, 1024, 2048 bits), DSA (512, 1024 bits)] that meet the following [assignment: PKCS #1 – RSA Encryption Standard (RSA), FIPS PUB 186-2 (DSA), FIPS PUB 180-1 (SHA1), RFC 1319 – The MD2 Message Digest Algorithm (MD2), RFC 1321 – The MD5 Message Digest Algorithm (MD5)].

FCS_COP.1.1_8

The TSF shall perform [assignment: *descifrado asimétrico*] in accordance with a specified cryptographic algorithm [assignment: *combinación de los algoritmos simétricos (DES, 3DES, AES, RC2, RC4) y los algoritmos asimétricos (RSA, DSA)*] and

cryptographic key sizes [assignment: *DES (56 bits), 3DES (168 bits), AES (128, 192, 256 bits), RC2 (40, 64, 128 bits), RC4 (128 bits), RSA (512, 1024, 2048 bits), DSA (512, 1024 bits)*] that meet the following [assignment: *PKCS #1 – RSA Encryption Standard (RSA), FIPS 46-3, Data Encryption Standard (DES/3DES), FIPS PUB 186-2 (DSA), FIPS PUB 197 (AES), RFC 2268 – A description of the RC2 Encryption Algorithm (RC2)*].

FPT – Protección del TSF

This class contains families of functional requirements that relate to the integrity and management of the mechanisms that provide the TSF (independent of TSP specifics) and to the integrity of TSF data (independent of the specific contents of the TSP data). In some sense, families in this class may appear to duplicate components in the FDP: User data protection class; they may even be implemented using the same mechanisms. However, FDP: User data protection focuses on user data protection, while FPT: Protection of the TSF focuses on TSF data protection. In fact, components from the FPT: Protection of the TSF class are necessary to provide requirements that the SFPs in the TOE cannot be tampered with or bypassed.

FPT_STM – Time Stamps

This family addresses requirements for a reliable time stamp function within a TOE.

FPT_STM.1 Reliable time stamps

Reliable time stamps, which require that the TSF provide reliable time stamps for TSF functions.

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

FDP – Protección de Datos de Usuario

This class contains families specifying requirements for TOE security functions and TOE security function policies related to protecting user data. FDP: User data protection is split into four groups of families that address user data within a TOE, during import, export, and storage as well as security attributes directly related to user data.

FDP_DAU – Data authentication

Data authentication permits and entity to accept responsibility for the authenticity of information (e.g., by digitally signing it). This family provides a method of providing a guarantee of the validity of a specific unit of data that can be subsequently used to verify that the information content has not been forged or fraudulently modified. In contrast to FAU: Security audit, this family is intended to be applied to "static" data rather than data that is being transferred.

FDP_DAU.1 Basic Data Authentication

Basic Data Authentication, requires that the TSF is capable of generating a guarantee of authenticity of the information content of subjects (e.g. documents).



FDP_DAU.1.1

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *la asociación entre los datos del usuario incluidos en una petición de certificación y la clave pública del usuario que solicita la certificación*].

FDP_DAU.2 Data Authentication with Identity of Guarantor

Data Authentication with Identity of Guarantor additionally requires that the TSF is capable of establishing the identity of the subject who provided the guarantee of authenticity.

FDP_DAU.2.1

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *la asociación entre los datos del usuario incluidos en una petición de certificación y la clave pública del usuario que solicita la certificación*].

Extensión de los requisitos funcionales de seguridad

Esta clase especifica requisitos funcionales para el entorno IT. La mayoría de ellos están extraídos del documento [CEN01c].

FPT – Protección de las TSF

Esta clase contiene familias de requisitos funcionales relativas a la integridad y a la gestión de los mecanismos provistos por las TSF (independientemente de las particularidades de las TSF) y a la integridad de los datos utilizados por las TSF (independientemente del contenido específico de estos datos). En un cierto sentido, puede parecer que las familias de esta clase duplican los componentes contenidos en FDP: clase sobre la protección de datos de usuario; pueden incluso estar implementados utilizando los mismos mecanismos. Sin embargo, FDP: La protección de los datos de usuario se focaliza en la protección de datos de usuario, mientras FPT: La protección de las TSF se focaliza en la protección de los datos de las TSF. De hecho los componentes de FPT: La clase para la protección de las TSF es necesaria para establecer requisitos sobre la imposibilidad de manipular o evitar las SFP del TOE

FPT_STM – Sellos de tiempo

Esta familia contempla requisitos sobre una función de sellado de tiempo fiable dentro del TOE.

FPT_STM.2 Sincronización de la hora

Las TSF deben contemplar instrucciones y requisitos relativos a la obtención fiable de la hora en aquellos servicios que sean dependientes de la hora

FPT_STM.2.1

Las TSF deben garantizar que todos los relojes de los TWSs que se utilicen para prestar los servicios CSP dependientes de la hora, están sincronizados con la siguiente

métrica [asignación: *difieren menos de 1 segundo de la hora universal coordinada (UTC)*].

FCS - Soporte criptográfico

Las TSF pueden utilizar funcionalidad criptográfica para ayudar a conseguir algunos objetivos de seguridad de alto nivel. Esto incluye (pero no está limitado a): identificación y autenticación, no repudio, ruta de confianza, canal de confianza y separación de datos. Esta clase se utiliza cuando el TOE implementa funciones criptográficas, la realización de las cuales puede estar en hardware, firmware y/o software

FCS_CKM - Gestión de claves criptográficas

Las claves criptográficas deben ser gestionadas a lo largo de su ciclo de vida. Esta familia está orientada a soportar este ciclo de vida y, en consecuencia, define requisitos para las siguientes actividades: generación de claves criptográficas, distribución de claves criptográficas, acceso a claves criptográficas y destrucción de claves criptográficas. Esta familia debe ser incluida cuando requisitos funcionales relativos a la gestión de claves criptográficas.

FCS_CKM.1 Generación de claves criptográficas

Este componente requiere que las claves criptográficas sean generadas de acuerdo a un algoritmo y a unos tamaños de clave específicos, los cuales pueden estar basados en un estándar asignado. Este componente también establece las condiciones de seguridad bajo las que se generan las claves criptográficas.

FCS_CKM.1.2

Las TSF deben garantizar que las claves de los tipos especificados [asignación: *claves* de firma de QC/NQC, claves de infraestructura y claves de control] sean generadas y almacenadas en un dispositivo de hardware criptográfico.

FCS_CKM.1.3

Las TSF deben garantizar que el dispositivo criptográfico seguro solamente genera claves de los tipos especificados [asignación: *claves de firma QC/NQC*] cuando se dan las siguientes condiciones [asignación: *como mínimo bajo el control de dos personas*].

FCS_CKM.3 Acceso a las claves criptográficas

Este componente requiere que el acceso a las claves criptográficas se realice según un método de acceso específico, el cual puede estar basado en un estándar asignado, y una protección adecuada de estas claves.

FCS_CKM.3.2

Las TSF deben garantizar que se realizan controles de acceso a todos los módulos criptográficos que utilizan claves de los tipos especificados [asignación: claves de firma *QC/NQC, claves de infraestructura y claves de control*].



FCS_CKM.4 Destrucción de claves criptográficas

Este componente establece que las claves criptográficas se destruyan según un método de destrucción específico, el cual puede basarse en un estándar asignado. Este componente también establece que las TSF incluyan las funciones apropiadas para la destrucción de claves comprometidas o de claves que alcancen el final de su vida operativa, con la finalidad de evitar el uso posterior de estas claves.

FCS_CKM.4.2

Las TSF deben garantizar que las claves de los tipos especificados [asignación: *claves de firma de QC/NQC*] sean destruidas cuando se den las siguientes condiciones [asignación: *alcanzan el final de su vida útil]*] de modo que las claves no puedan ser recuperadas.

FCS_CKM.4.3

Las TSF deben asegurar que se destruyan las claves de los tipos específicos [asignación: *claves secretas/privadas]* de aquellos dispositivos que se hayan utilizado para generar, utilizar o almacenar las claves y que vayan a ser retirados del servicio o transferidos.

FCS_CKP - Protección de claves criptográficas

Las TSF deben establecer requisitos de seguridad para proteger y distribuir la clave pública del servicio de generación de certificados QC/NQC, la claves de infraestructura y las claves de control. Debido a las diferentes amenazas sobre las claves de los TWSs, que dependen de dónde y cómo son utilizadas, es importante clasificar las claves de acuerdo a su perfil de riesgo.

FCS_CKP.1 Mecanismos de seguridad aplicados a las claves criptográficas

Este componente requiere la protección de la clave pública del servicio de generación de certificados QC/NQC, de la claves de infraestructura, de las claves control y de las claves de sujeto

FCS_CKP.1.1

Las TSF deben ser capaces de [selección, elegir uno de: *evitar*] la intercepción o manipulación de las claves públicas que no hayan sido certificadas.

FCS_CKP.2 Protección de la distribución de claves

Este componente requiere la protección de la distribución de la clave pública del servicio de generación de certificados QC/QNC, de las claves de infraestructura y de las claves de control, y mecanismos de protección aplicables a la exportación de claves

FCS_CKP.2.1

Las TSF no distribuirán en claro los tipos de claves especificados [asignación: *claves privadas y secretas*].

FCS_CKP.2.2

Las TSF deben garantizar que cualquier clave sensible nunca se almacena de forma desprotegida. Si las claves de los tipos especificados [asignación: *cualquier clave privada/secreta*] se exportan del módulo en el que están almacenadas, entonces e el módulo debe proteger a dichas claves antes de que salgan de él, para asegurar su confidencialidad. Si las claves de los tipos especificados se protegen mediante cifrado, entonces las TSF cifrarán dichas claves de acuerdo a un algoritmo criptográfico especificado que cumpla con lo siguiente [asignación: *requisitos criptográficos especificados en [ALGO]*].

FCS_CKP.3 Almacenamiento, copia de seguridad y recuperación de claves

Este componente requiere que las TSF garanticen que las funciones para la realización de copias de seguridad de claves y para su recuperación sigan un método específico.

FCS_CKP.3.1

Las TSF deben garantizar que las claves de los tipos especificados [asignación: *todas las claves privadas/secretas, claves privadas/secretas de infraestructura y de control*] se guardan utilizando un mecanismo de almacenamiento especificado [asignación: *cualquier mecanismo seguro para claves privadas/secretas, un dispositivo de hardware criptográfico para claves privadas/secretas de infraestructura y de control*].

FCS_CKP.3.2

Las TSF deben garantizar que la copia de seguridad, el almacenamiento y la recuperación de claves de los tipos especificados [asignación: *claves privadas de firma NQC/QC, claves de infraestructura, claves de control*] solamente se realizan por [asignación: *personal autorizado*] cuando se dan las siguientes condiciones [asignación: *como mínimo bajo el control de dos personas para claves privadas de firma NQC/QC*].

FCS_KCH - Cambio de claves criptográficas

Un CSP que utiliza TWSs necesita garantías y requisitos de seguridad relativos al cambio de claves. El cambio de claves puede ser:

- Programado, en el que una clave se reemplaza por otra nueva cuando la primera alcanza el final de su vida operativa (según determine la política)
- No programado, en el que una clave se reemplaza por otra nueva, si la primera ha sido comprometida.

FCS_KCH.1 Garantías en el cambio de claves

Este componente requiere un mecanismo para poder cambiar las claves de manera segura.

FCS_KCH.1.1

El TSF debe garantizar que las claves de los tipos especificados [asignación: *claves de infraestructura y claves de control*] se cambian de forma regular, e.g. anualmente.



FCS_KCH.1.2

Las TSF deben asegurar que el cambio se realice de forma segura y que éste pueda realizarse tanto *online* como *offline*.

XR - Servicio de registro

Esta clase proporciona dos familias que proporcionan los requisitos de seguridad que necesita un servicio de registro. El servicio de registro verifica la identidad y, si procede, cualesquiera atributos específicos de un sujeto. Los resultados de este servicio se pasan al servicio de generación de certificados. Las familias que se incluyen en esta clase soportan la disponibilidad de los mecanismos de seguridad requeridos, tales como la protección de las peticiones de certificación o la protección de los datos del sujeto.

XR_SDM - Gestión de datos de sujeto

Esta familia define requisitos de seguridad que son necesarios para proteger la información sobre los sujetos.

XR_SDM.1 Gestión de los datos de sujeto

Con este componente, las TSF incorporan los requisitos necesarios para proteger la información sobre los sujetos.

XR_SDM.1.1

Las TSF deben garantizar la capacidad de implementar mecanismos y controles de seguridad para proteger la privacidad y confidencialidad de los datos sobre los sujetos.

XCG - Servicio de generación de certificados

La finalidad de esta clase es especificar la gestión de varios aspectos del servicio de generación de certificados. Este servicio crea y firma certificados que se basan en la identidad y demás atributos de un sujeto, según lo verificado por el servicio de registro.

Esta clase proporciona dos familias las cuales soportan los procesos relacionados con la generación de certificados y los requisitos funcionales asociados a la renovación de certificados.

XCG_CGE - Generación de certificados

Esta familia define requisitos de seguridad sobre la generación de certificados. Después de recibir una petición de certificado a través del servicio de registro, los TWSs generan un certificado de la clave pública suministrada. Esto asegura que el CSP blinde el vínculo entre la clave pública del sujeto y la identidad de éste.

Los TWSs también pueden enviar las claves públicas de control y de infraestructura para que sean certificadas por el servicio de generación de certificados. Esto resulta en la producción de certificados de infraestructura y de certificados de control.



Después de generar un certificado, éste puede entregarse a través de un dispositivo suplementario de provisión a sujetos o bien puede darse directamente al sujeto.

Los certificados de control y de infraestructura pueden proporcionarse directamente al componente confiable que requiere su uso.

XCG_CGE.1 Procesado de peticiones de certificación

Con este componente, las TSF incorporan requisitos de seguridad sobre el procesamiento de peticiones de certificación.

XCG_CGE.1.1

Las TSF deben asegurar que el servicio de generación de certificados garantiza la [selección: *integridad, autenticidad del origen de los datos, privacidad y confidencialidad*] del mensaje de petición de certificado.

XCG_CGE.2 Garantías de los certificados emitidos

Con este componente, las TSF incorporan garantías y propiedades relacionadas con los certificados emitidos.

XCG_CGE.2.2

Las TSFs deben garantizar que los certificados emitidos por los TWS tengan las siguientes propiedades [asignación: *indicación del nombre o pseudónimo del sujeto; en el caso de que se utilice un pseudónimo esto deberá indicarse claramente . La clave pública del certificado está relacionada con la clave privada del sujeto. La firma electrónica avanzada del CSP, creada mediante la utilización de las claves de firma del CSP. El certificado debe contener un número de serie distinto y único asignado por el TWS; debe ser único con respecto al CSP emisor. El certificado debe especificar un valor de inicio de su validez que no sea anterior al instante de su emisión y un valor de fin de validez que no preceda al del inicio de validez. Las claves/algoritmos de firma utilizados por el TWS para firmar el certificado deben ser conformes con el estándar [ALGO] sobre especificaciones de algoritmos. El certificado debe incluir una referencia a la política de certificación bajo la cual es emitido*].

XCG_CGE.2.3

Las TSF deben asegurar que los certificados cualificados emitidos por el TWS sean conformes a lo siguiente [asignación: *especificación [TS101862]*].

XCG_CRE - Renovación de certificados

Esta familia define requisitos de seguridad sobre la renovación de certificados. Un certificado pueden renovarse dentro del período previo a su expiración, siendo este período el que defina la política aplicable. La renovación de certificados puede consistir en un escenario de re-emisión de claves: una clave pública nueva se certifica utilizando información de registro utilizada para generar el certificado previo.

La renovación de certificados abarca los certificados de firma QC/QNC, los certificados de infraestructura, los certificados de control y los certificados de sujeto.



XCG_CRE.1 Renovación de certificados de entidades que no son sujetos

Con este componente las TSF incorporan requisitos de seguridad sobre el proceso de renovación de certificados de firma QC/QNC, de certificados infraestructura y de certificados de control.

XCG_CRE.1.1

Las TSF deben garantizar que las claves de los tipos especificados [asignación: *claves de firma QC/NQC*] se renuevan antes de que expiren y bajo las siguientes condiciones [asignación: *las correspondientes claves públicas renovadas proporcionan al menos el mismo nivel de confianza que cuando fueron inicialmente distribuidas*].

XCG_CRE.2 Renovación de certificados de entidades que son sujetos

Con este componente las TSF incorporan requisitos de seguridad sobre el proceso de renovación de certificados de sujeto.

XCG_CRE.2.1

Las TSF deben garantizar que el mecanismo que se utiliza para [selección, elegir uno de: regeneración de claves*] de claves de sujeto cumple con las siguientes condiciones [asignación:* debe ser igual de seguro que la generación del certificado inicial]

XRM - Servicio de gestión de la revocación de certificados

La finalidad de esta clase es especificar la gestión de varios aspectos del servicio de gestión de la revocación y del servicio de estado de revocación.

El servicio de gestión de la revocación se encarga de procesar las peticiones y los reportes relativos a la revocación para determinar las acciones necesarias que deben llevarse a cabo. Los resultados de este servicio se distribuyen mediante el servicio de estado de revocación.

El servicio de estado de revocación proporciona información de estado de revocación a interlocutores dependientes. Este servicio puede ser un servicio en tiempo real o puede estar basado en información de estado de revocación que se actualiza a intervalos regulares.

Esta clase proporciona dos familias que soportan el proceso relacionado con las peticiones de cambio de estado de certificados, y los procesos relacionados con la revocación/suspensión de certificados.

XRM_CSC - Peticiones de cambio de estado de certificados

Esta familia define requisitos de seguridad sobre las peticiones de cambio de estado de certificados. Cuando un sujeto sospecha que su clave privada puede haber sido comprometida, debe enviar a los TWS de su CSP una petición de suspensión (revocación temporal) de su certificado. El sujeto también podrá realizar la correspondiente petición para reestablecer la operatividad del certificado.

Cuando el sujeto conoce que su clave privada ha sido efectivamente comprometida, envía una petición de revocación de su certificado a los TWS de su CSP.

El CSP también puede solicitar cambios de estado de certificados a través de este servicio. El estado de los certificados de control y de los certificados de infraestructura se puede controlar también a través de este servicio. Las peticiones para cambiar el estado de un certificado son mensajes autenticados que pueden ser aceptados o rechazados por el CSP.

XRM_CSC.1 Requisitos de seguridad sobre peticiones de revocación

Con este componente, las TSF incorporan requisitos de seguridad sobre el procesamiento de peticiones de cambio de estado de certificados.

XRM_CSC.1.3

Las TSF deben garantizar que la revocación de certificados que correspondan a claves de firma de QC/QNC sólo sea posible bajo las siguientes condiciones [asignación: *bajo el control de dos personas, como mínimo*].

XRS - Servicio de estado de revocación de certificados

Esta clase proporciona dos familias, las cuales contienen los requisitos de seguridad sobre el servicio de estado de revocación de certificados.

El servicio de estado de revocación proporciona información sobre el estado de revocación de certificados a los interlocutores dependientes. Este servicio puede ser un servicio en tiempo real o puede estar basado en información de estado de revocación que se actualiza a intervalos regulares. El servicio de estado de revocación debe obtener información fiable de la base de datos de estados de certificado, en la que los procesos de gestión de la revocación insertan la información de estados de certificado.

Las familias incluidas en esta clase soportan la disponibilidad de mecanismos de seguridad necesarios como la protección de las peticiones y respuestas de estado, o la protección de la comunicación entre el proceso de gestión de la revocación y el servicio de estado de revocación.

El servicio de estado de revocación puede ser un servicio *online* (que proporciona el estado del certificado en tiempo real) o un servicio *offline* (en el que el estado del certificado no es en tiempo real).

Donde sea un servicio *online*, un interlocutor dependiente, se comunicará con el servicio de estado de revocación y éste le proporcionará los detalles del o de los certificados cuyo estado pregunte. El servicio de estado de revocación *online*, cuando utilice un sistema de envío de mensajes en tiempo real, realizará una consulta a la base de datos de estados de certificado para obtener el estado actual del certificado que se solicite o, si utiliza el envío periódico de mensajes, consultará sus registros internos, los cuales habrán sido actualizados por el último mensaje periódico. De este modo se crea una respuesta y se envía al interlocutor dependiente indicando el estado del o de los certificados solicitados. Donde sea un servicio *offline* el servio de estado de revocación mantendrá el mensaje periódico más reciente. Éste podría ser obtenido por el interlocutor dependiente para comprobar el estado de un certificado.



XRS_RSD - Datos de estado de revocación

Esta familia define requisitos de seguridad sobre la comunicación entre el servicio de estado de revocación y el servicio de gestión de revocación. Esta comunicación consiste en la transferencia de información de estado de certificados desde la base de datos de estados de certificado al servicio de estado de revocación.

El servicio de estado de revocación proporciona información sobre el estado de revocación de certificados a los interlocutores dependientes. El servicio de estado de revocación refleja los cambios de estado de certificado producidos a partir de peticiones de cambio procedentes tanto del titular, como del CSP, como de un tercero y que han sido procesadas por el servicio de gestión de la revocación. Estos datos también pueden ponerse a disposición de los titulares de certificados si la política requiere que los titulares tengan acceso a los datos de estado de revocación.

XRS_RSD.1 Confianza del servicio de estado de revocación

Con este componente se incorporan restricciones sobre la confianza del servicio de estado de revocación.

XRS_RSD.1.1

Las TSF deben garantizar que [selección: *los mensajes periódicos*] proporcionados al servicio de estado de revocación proceden únicamente de servicios de gestión de la revocación que son de confianza.

XTS - Servicio de sellado de tiempo

Esta clase proporciona dos familias que soportan los mecanismos de seguridad necesarios para el servicio de sellado de tiempo.

Una autoridad de sellado de tiempo (TSA) es una tercera parte de confianza que proporciona un servicio de sellado de tiempo, i.e de generación de sellos de tiempo, los cuales pueden servir como prueba de que ciertos datos existían con anterioridad a un determinado instante de tiempo(prueba de existencia).

Un servicio de sellado de tiempo proporciona un proceso de sellado de tiempo, el cual vincula criptográficamente instantes de tiempo a datos.

XTS_REC - Corrección de las peticiones de sellado de tiempo

Esta familia define requisitos de seguridad sobre la corrección y completitud de las peticiones. Si el resultado de las funciones correspondientes es positivo, los datos se enviarán como entrada de las funciones de generación de sellos de tiempo.

XTS_REC.1 Verificación del origen de la petición

Con este componente, las TSF incorporan restricciones sobre la verificación del origen de las peticiones.

XTS_REC.1.1

Las TSF deben proveer funciones para controlar el origen de cada petición antes de comprobar su corrección, utilizando los mecanismos de seguridad especificados [asignación: *mecanismo de autenticación del origen de los datos*]

XTS_REC.2 Verificación de los algoritmos de la petición

Con este componente, las TSF incorporan requisitos relativos a la verificación de los algoritmos criptográficos utilizados en la petición.

XTS_REC.2.1

Las TSF deben garantizar que la TSA verifica que la petición de sellado de tiempo utiliza un algoritmo de *hash* que satisface lo siguiente [asignación: *está especificado como aprobado por [ALGO]*].

XTS_REG - Generación de respuestas de sellado de tiempo

Comportamiento de la familia

Esta familia define los requisitos de seguridad necesarios para generar respuestas de sellado de tiempo.

Esta familia define funciones para los siguientes propósitos:

- Generación de parámetros de tiempo. Estas funciones utilizan una fuente fiable para entregar parámetros de tiempo que sean precisos. Estos parámetros se utilizan como entrada del proceso de generación de sellos de tiempo.
- Generación de sellos de tiempo. Estas funciones son responsables de la creación de un sello de tiempo que vincula la hora vigente, un número de serie único y los datos proporcionados para el sellado, asegurando que se observan todos los requisitos de la política.
- Computación del sellado de tiempo. Estas funciones computan el sello de tiempo que se devuelve al cliente. Estas funciones firman criptográficamente los datos proporcionados por la función de generación de sellos de tiempo.

XTS_REG.1 Generación de parámetros de tiempo

Con este componente las TSF incorporan requisitos sobre la necesidad de incluir un en las respuestas de sellado de tiempo valores de tiempo que se hayan obtenido de una fuente fiable.

XTS_REG.1.1

Las TSF deben garantizar que la fuente de valores de tiempos de confianza de la TSA esté sincronizada con la siguiente métrica [asignación: *difiere menos de 1 segundo de la hora universal coordinada (UTC), con una tolerancia establecida por la política*].



XTS_REG.1.2

Las TSF deben garantizar que el reloj de la TSA se sincroniza con lo siguiente [asignación: *UTC*], utilizando un mecanismo que satisface lo siguiente [asignación: *se ha demostrado ser fiable*].

XTS_REG.2 Contenido de una respuesta de sellado de tiempo

Con este componente, las TSF incorporan requisitos sobre los datos que es necesario incluir en el contenido de las respuestas de sellado de tiempo.

XTS_REG.2.2

Las TSF deben garantizar que el TST incluye la precisión de la fuente de tiempo utilizada cuando ocurran las siguientes condiciones [asignación: *si excede la que la política de la TSA requiere*].

XTS_REG.3 Garantías de seguridad de las respuestas de sellado de tiempo

Con este componente, las TSF incorporan requisitos que son necesarios para garantizar la seguridad de los sellos de tiempo que se generen.

XTS_REG.3.2

Las TSF deben garantizar que las claves de los tipos especificados [asignación: *claves de firma de la TSA, claves de control de la TSA*], que pertenezcan a la TSA deben generarse y guardarse en un dispositivo de hardware criptográfico.

XSP - Servicio de entrega de dispositivos a sujetos

La finalidad de esta clase es especificar la gestión de varios aspectos del servicio de entrega de dispositivos a sujetos. Este servicio se considera como un servicio suplementario y opcional de un CSP.

El servicio de entrega de dispositivos a los sujetos, prepara y proporciona dispositivos de creación de firma (SCDev) a los sujetos. Ejemplos de este servicio son:

- Un servicio que genera los pares de claves de los sujetos y les proporciona las claves privadas.
- Un servicio que prepara los dispositivos de creación de firma segura de los sujetos (SSCD) y los códigos activadores de dichos dispositivos y los entrega a los sujetos registrados.

Este servicio puede proporcionar un SCDev y/o un SSCD. Los requisitos de seguridad aplicables a los SCDs también son aplicables a los SSCDs, donde los SSCDs cumplen los requisitos adicionales que se establecen en el Anexo III de [Eur99a]. No se hace ninguna distinción respecto a si el SCDev/SSCD se implementa en hardware o en software.

XSP_ACD - Creación y distribución de los datos de activación

Esta familia define los requisitos de seguridad aplicables a la creación y distribución de los datos de activación. Los SCDev y su contenido están protegidos con datos



secretos de activación. El CSP es responsable de la generación de estos datos de activación y de su posterior distribución segura a los sujetos.

XSP_ACD.1 Garantías de la creación y distribución de datos de activación

Con este componente, las TSF incorporan requisitos de seguridad sobre los procesos de creación y distribución de datos de activación.

XSP_ACD.1.2

Las TSF deben garantizar que los datos de activación iniciales son generados de forma segura.

XAA – Responsabilidad y auditoría

Esta clase define requisitos de seguridad sobre el registro de la ocurrencia de eventos de seguridad relevantes que tienen lugar bajo el control de las TSF. Esta clase proporciona dos familias que soportan los procesos relacionados con la auditoría de los eventos.

XAA_RAR – Restricción de la revisión de auditoría

Esta familia define requisitos de seguridad que se aplican a la protección de los datos de auditoría.

XAA_RAR.1 Integridad de los datos de auditoría

Con este componente, las TSF incorporan requisitos de seguridad sobre la necesaria integridad de los datos de auditoría.

XAA_RAR.1.1

Las TSF serán capaces de [selección, elegir uno de: evitar] la modificación de los registros de auditoría.

XAA_GAT – Garantías del tiempo de los registros de auditoría

Esta familia define requisitos de seguridad sobre el tiempo que se utiliza para marcar la hora de los registros de auditoría.

XAA_GAT.1 Tiempo de confianza en los datos de auditoría

En este componente, las TSF incorporan garantías sobre la hora que se utiliza para marcar los eventos auditados.

XAA_GAT.1.1

Las TSF deben garantizar que una fuente confiable de tiempo que satisface los siguiente [asignación: *garantías requeridas por el requisito FPT_STM.2.1*] se utilizará para marcar el tiempo de los eventos auditados.



XBK – Copias de seguridad y recuperación

Esta clase define los requisitos de seguridad sobre copias de seguridad y recuperación de todas la informaciones del sistema, informaciones de los sujetos y cualesquiera otros datos que sean necesarios para restablecer el sistema después de un fallo o de un desastre. Esta clase no abarca la copia de seguridad y la recuperación de claves.

XBK_BAR – Copia de seguridad y recuperación

Esta familia define requisitos de seguridad sobre las copias de seguridad y los procesos de recuperación.

XBK_BAR.1 Generación de copias de seguridad

Con este componente, las TSF incorporan requisitos de seguridad sobre la generación de copias de seguridad de la información necesaria para restablecer el sistema después de un fallo o de un desastre.

XBK_BAR.1.1

Las TSF deben incluir una función de copia de seguridad que almacene los datos que sean suficientes para recrear el estado del sistema.

XBK_BAR.1.2

Las TSF deben garantizar que la función de copia de seguridad sólo puede ser utilizada por los usuarios especificados [asignación: *usuarios con un rol con los suficientes privilegios*].

XBK_BAR. Recuperación

Con este componente, las TSF incorporan requisitos de seguridad sobre el proceso de restablecimiento después de un fallo o de un desastre.

XBK_BAR.2.1

Las TSF deben incluir una función de recuperación para restablecer el estado del sistema a partir de una copia de seguridad.

XBK_BAR.2.2

Las TSF deben garantizar que la función de recuperación sólo puede ser utilizada por los usuarios [asignación: *usuarios con un rol con los suficientes privilegios*].

Extensión de los requisitos sobre garantía de la seguridad

XSO: Sistemas y operaciones

Esta clase proporciona dos familias que se ocupan específicamente de garantizar la operación segura de los TWS y de la gestión fiable de los valores de tiempo que las TSF utilizan.



XSO_OPM Gestión de las operaciones

Un CSP que utiliza TWSs necesita garantizar que las funciones de gestión de las operaciones son convenientemente seguras.

Dependencias

AGD_ADM.1 Guía del Administrador

ADO_IGS.1 Procedimientos de Instalación, generación y puesta en marcha

Acciones del desarrollador

El desarrollador debe documentar los procedimientos necesarios para la operación segura del TOE.

Contenido y presentación de las evidencias

La documentación debe describir los pasos necesarios para la operación segura del TOE.

Acciones del evaluador

El evaluador debe confirmar que la información suministrada cumple los requisitos de contenido y presentación de las evidencias.

El evaluador debe determinar que los procedimientos operativos resultan en una configuración segura.

XSO_OPM.1.1:

Los TWS deben proporcionar instrucciones que permitan que el CSP sea:

- Utilizado de forma correcta y segura
- Desplegado de forma que se minimice el riesgo de fallo de los sistemas.

CAPÍTULO 6

Especificación resumida del TOE

Esta especificación resumida, contiene:

- Una declaración de las funciones de seguridad del TOE, que abarca las funciones de seguridad IT y que especifica cómo estas funciones satisfacen los requisitos funcionales de seguridad del TOE.
- Una declaración de las medidas de garantía, que muestra cómo se satisfacen los requisitos de garantía.

Funciones de seguridad del TOE

En esta sección se proporciona una descripción de las funciones de seguridad del TOE que cumplen con la seguridad exigida al TOE.

Finalmente, la última sección (sección Tabla de asociación entre requisitos funcionales y funciones de seguridad) incluye una tabla que cruza los requisitos funcionales de seguridad del TOE que se incluyen los estos Objetivos de Seguridad y las funciones de seguridad del TOE que se especifican en el documento.

FAU – Auditoría de la seguridad

FAU_GEN.1.1

El sistema KeyOne puede generar un registro de auditoría con los siguientes eventos:

a) Arranque y parada de las funciones de auditoría (no aplicable[3]).

b) [Los siguientes eventos:

- *Éxitos y fallos en la actividad de la aplicación (después de que el usuario de la aplicación haya sido correctamente identificado y autenticado y que la aplicación haya comenzado).*

[3] *Las funciones de auditoría no son parte separada del producto, sinó que este componente está integrado en el conjunto de funcionalidad de los productos..*



- Emitir un sello de tiempo.
- Procesar una petición de certificación/revocación/regeneración de claves.
- Aprobación de peticiones para certificación/revocación/regeneración de claves.
- Registro, incluyendo las peticiones de regeneración de claves.
- *Inicio/finalización de sesiones de las siguientes aplicaciones: KeyOne CA, KeyOne TSA y KeyOne VA.*
- Generación de una CRL.
- Cancelación del procesamiento de un lote.
- All certificate status requests and responses received/sent by the online Revocation Status Service.
- Todas las peticiones y respuestas de estado de certificado recibidas/enviadas por el servicio de estado de revocación.
- Todos los sellos de tiempo generados por el servicio de sellado de tiempo.]

Para almacenar información (registros de auditoría) en la base de datos de cualquier aplicación KeyOne, se requiere utilizar la API de base de datos i3D. La inserción de un registro de auditoría implica la inserción de un registro lógico de i3D. Esta inserción añade los siguientes dos registros:

- Un registro en la tabla de histórico de registros (registro histórico) que contiene codificados en DER los datos que hay que almacenar (campo `info`) y otros campos de control. El nuevo registro incluye la información del identificador de la sesión activa (campo `sessionid`). El registro en su totalidad se firma simétricamente utilizando la clave de sesión (campo `hmac`).
- Un registro en la tabla de consultas que está asociado al registro histórico (a través del campo `hmac`). Ese registro contiene, en columnas no codificados, algunos de los datos del registro lógico que se almacena. Estas columnas son las siguientes:
  - **Fecha y hora** en la que ocurrió el evento. La fecha/hora se representa en (`time_t`) formato numérico (columna `timelog`).
  - **Nombre distinguido de la entidad** que provocó el evento (campo `author`). Corresponde con el nombre distinguido del PSS que se estaba en uso cuando se realizó la operación. El nombre distinguido se representa como una cadena de caracteres de acuerdo al formato que se define en [RFC2253].
  - Una cadena de caracteres que indica el **tipo de entidad** que provocó el evento (columna `role`). Corresponde con el valor del atributo role del PSS que estaba en uso cuando se realizó la operación.
  - Un número que indica el **tipo de evento** (columna `evtype`).

- Un número que identifica unívocamente al evento dentro del conjunto de eventos del mismo tipo que son generados por el mismo módulo (columna `event`).

- Un número que identifica el **módulo** que generó el evento (columna `modu`). Esta columna contiene un valor nulo para los eventos del tipo MARCA.

- Un número que indica la **importancia del evento** (campo `evlevel`). Los registros de evento se clasifican en las siguientes categorías, según su importancia:

  - Informativo: Los eventos de esta categoría informan de operaciones que se culminaron con éxito. Esta categoría implica una operación realizada correctamente.

  - Marca: Los eventos de esta categoría se registran cuando comienza una sesión de administración y cuando finaliza. Esta categoría implica una operación realizada correctamente.

  - Advertencia: Indica la detección de una condición inusual al realizar una operación pero que no provocó el fallo de la misma. Esta categoría implica un fallo en una operación.

  - Error: Indica que una operación falló debido a un error predecible: Esta categoría implica una operación fallida.

  - Error fatal: Indica que durante una operación ocurrió una circunstancia excepcional no predecible. Esta categoría implica una operación fallida.

- Una cadena de caracteres que **describe el evento**. Para algunos eventos, la descripción va seguida de una lista de parámetros (separados por caracteres de salto de línea) cuyo valor varía dependiendo de los datos sobre los que se realizó la operación (columna `obser`).

- Un número que indica el **nivel de anidamiento del evento** (columna `indlevel`). Los eventos que producen algunas operaciones se organizan jerárquicamente de forma que un evento puede agrupar a otros de nivel inferior. Para los eventos del primer nivel, esta columna contendrá el valor 1, Para eventos de segundo nivel y superiores, el valor será mayor que 1. El valor 0 se almacenará para aquellos eventos en los que esta característica no sea aplicable.

Las secciones `Screen for browsing logs in KeyOne CA and KeyOne TSA applications` y `Screen for browsing logs in KeyOne VA application` del capítulo `Security Audit` del documento [FUNCSPEC], especifican todos los detalles sobre la información que se reporta cuando los registros de auditoría se consultan a través de las aplicaciones KeyOne. Estas secciones demuestran el almacenamiento de la información que se especifica en este requisito.

Además el sistema KeyOne es capaz de generar archivos en medios adecuados para el almacenamiento y el posterior procesamiento, cuando sea necesario proporcionar evidencias legales como soporte de las firmas digitales.



Los componentes KeyOne CA, KeyOne VA y KeyOne TSA generan archivos con los datos que gestionan y procesan. Estos archivos se basan en una base de datos que se encuentra en el disco duro del *host* que mantiene esta información.

Todas la informaciones que el sistema gestiona está almacenada en la base de datos de la aplicación lo cual es conforme con el servicio de archivado porque los datos históricos son mantenidos en la base de datos de explotación

Todos los registros de base de datos se almacenan en la base de datos de los componentes KeyOne. El servicio de generación de datos de archivo se consigue también de acuerdo al procedimiento descrito en el apéndice CPS de KeyOne 2.1.

Consecuentemente esta función está relacionada con la generación de archivos en los componentes KeyOne (base de datos) y por lo tanto esta función está implicada en las operaciones SQL que se realizan sobre la base de datos.

Las aplicaciones KeyOne deben acceder su base de datos asociada a través de la API i3D. La API de base de datos i3D es una interfaz Scryptor para acceder bases de datos i3D. Esta API toma la forma de un objeto de Scryptor (i3DHandler), que proporciona métodos para establecer asociaciones con tablas lógicas i3D, de forma que es posible añadir, modificar y consultar los registros lógicos escondiendo los detalles de la tecnología i3D de las tablas físicas subyacentes. Las operaciones SQL se pueden realizar sobre los registros de las tablas lógica y las funciones criptográficas se ejecutarán para aplicar los mecanismos de seguridad i3D.

En relación a la generación de sellos de tiempo por parte del servicio de sellado de tiempo, KeyOne TSA genera archivos con los datos que gestiona y procesa. Estos archivos se basan en una base de datos que se encuentra en el disco duro de un *host* que mantiene esta información. Todos los sellos de tiempo que genera el sistema KeyOne se almacenan en la tabla `tsa_traces` de la base de datos de KeyOne TSA. Esta tabla contiene todos los mensajes enviados y recibidos por el servidor de TSA; así, debido a que los mensajes que la TSA envía contienen los TST que han sido generados por la TSA, éstos resultan también guardados en los archivos de KeyOne TSA.

FAU_GEN.1.2

The KeyOne system records within each audit record the following information:

El sistema KeyOne registra dentro de cada registro de error la siguiente información:

- Hora y fecha del evento[4], tipo del evento[5], identidad del sujeto[6], y el resultado (éxito o fracaso) del evento[7]; y
- Para cada tipo de evento de auditoría, basada en las definiciones de eventos de los componentes funcionales incluidos en el ST, la siguiente información adicional: role de la identidad del sujeto[8], nivel del evento[9] (eventos anidados),

---

[4] *Campo `Timelog` de la tabla de registros de auditoría.*
[5] *Campo `Evtype` de la tabla de registros de auditoría.*
[6] *Campo `Author` de la tabla de registros de auditoría.*
[7] *Campo `Evlevel` de la tabla de registros de auditoría.*
[8] *Campo `Role` de la tabla de registros de auditoría.*
[9] *Campo `Indlevel` de la tabla de registros de auditoría.*



categoría del evento[10], observaciones[11] (más información sobre el evento), identificador del evento[12], datos de certificación y datos de revocación.

Para almacenar información (registros de auditoría) en la base de datos de cualquier aplicación KeyOne, se requiere utilizar la API de base de datos i3D. La inserción de un registro de auditoría implica la inserción de un registro lógico de i3D. Esta inserción añade los siguientes dos registros:

- Un registro en la tabla de histórico de registros (registro histórico) que contiene codificados en DER los datos que hay que almacenar (campo `info`) y otros campos de control. El nuevo registro incluye la información del identificador de la sesión activa (campo `sessionid`). El registro en su totalidad se firma simétricamente utilizando la clave de sesión (campo `hmac`).
- Un registro en la tabla de consultas que está asociado al registro histórico (a través del campo `hmac`). Ese registro contiene, en columnas no codificados, algunos de los datos del registro lógico que se almacena. Estas columnas son las siguientes:
  - **Fecha y hora** en la que ocurrió el evento. La fecha/hora se representa en (`time_t`) formato numérico (columna `timelog`).
  - **Nombre distinguido de la entidad** que provocó el evento (campo `author`). Corresponde con el nombre distinguido del PSS que se estaba en uso cuando se realizó la operación. El nombre distinguido se representa como una cadena de caracteres de acuerdo al formato que se define en [RFC2253].
  - Una cadena de caracteres que indica el **tipo de entidad** que provocó el evento (columna `role`). Corresponde con el valor del atributo role del PSS que estaba en uso cuando se realizó la operación.
  - Un número que indica el **tipo de evento** (columna `evtype`).
  - Un número que identifica unívocamente al evento dentro del conjunto de eventos del mismo tipo que son generados por el mismo nódulo (columna `event`).
  - Un número que identifica el **módulo** que generó el evento (columna `modu`). Esta columna contiene un valor nulo para los eventos del tipo MARCA.
  - Un número que indica la **importancia del evento** (campo `evlevel`). Los registros de evento se clasifican en las siguientes categorías, según su importancia:
    - Informativo: Los eventos de esta categoría informan de operaciones que se culminaron con éxito. Esta categoría implica una operación realizada correctamente.
    - Marca: Los eventos de esta categoría se registran cuando comienza una sesión de administración y cuando finaliza. Esta categoría implica una operación realizada correctamente.

---

[10] Campo `Modu` de la tabla de registros de auditoría.
[11] Campo `Obser` de la tabla de registros de auditoría.
[12] Campo `Event` de la tabla de registros de auditoría.



  - Advertencia: Indica la detección de una condición inusual al realizar una operación pero que no provocó el fallo de la misma. Esta categoría implica un fallo en una operación.

  - Error: Indica que una operación falló debido a un error predecible: Esta categoría implica una operación fallida.

  - Error fatal: Indica que durante una operación ocurrió una circunstancia excepcional no predecible. Esta categoría implica una operación fallida.

- Una cadena de caracteres que **describe el evento**. Para algunos eventos, la descripción va seguida de una lista de parámetros (separados por caracteres de salto de línea) cuyo valor varía dependiendo de los datos sobre los que se realizó la operación (columna `obser`).

- Un número que indica el **nivel de anidamiento del evento** (columna `indlevel`). Los eventos que producen algunas operaciones se organizan jerárquicamente de forma que un evento puede agrupar a otros de nivel inferior. Para los eventos del primer nivel, esta columna contendrá el valor 1, Para eventos de segundo nivel y superiores, el valor será mayor que 1. El valor 0 se almacenará para aquellos eventos en los que esta característica no sea aplicable.

Puesto que cuando un evento se registra, dichos campos son archivados, entonces la asociación entre cada evento y la identidad del usuario que provocó el evento queda almacenada.

Las secciones `Screen for browsing logs in KeyOne CA and KeyOne TSA applications` y `Screen for browsing logs in KeyOne VA application` del capítulo `Security Audit` del documento [FUNCSPEC], especifican todos los detalles sobre la información que se reporta cuando los registros de auditoría se consultan a través de las aplicaciones KeyOne. Estas secciones demuestran el almacenamiento de la información que se especifica en este requisito.

Por lo tanto, el sistema KeyOne mantiene un archivo de los datos que gestiona la aplicación; los siguientes elementos son archivados:

- Todos los certificados;

- Todas las CRLs/ARLs;

- Todos los registros de auditoría.

La base de datos gestionada por el sistema KeyOne archiva informaciones diversas, dependiendo con el tipo de componente con el que está relacionado.

Certificados

Todos los certificados que el sistema KeyOne genera, se almacenan en la tabla `cert_ca` que hay en la base de datos de KeyOne CA. Esta tabla es utilizada por KeyOne CA para almacenar todos los certificados que emite.

Las columnas de esta tabla son las siguientes:

- `status` (tipo SQL: int): Un número que identifica el estado del certificado.

- `reqtype` (tipo SQL: char 65): Una cadena de caracteres que indica los tipos de la petición-respuesta (ambos separados por un guión) de la petición a partir de la cual el certificado se generó. Para los certificados que resultan del procesado de peticiones de certificado individuales realizadas desde la aplicación de administración de KeyOne CA, esta columna contiene el valor nulo.

- `Timereq` (tipo SQL: int): Para certificados generados a partir de lotes de peticiones, esta columna contiene la fecha y la hora en la que el lote fue generado por la RA. Para certificados que resultan del procesado de peticiones de certificación individuales, esta columna indica la hora en la que la petición fue procesada por KeyOne CA. La fecha/hora se almacena en formato numérico (`time_t`).

- `notbefore` (tipo SQL: int): La fecha en la que comienza la validez del certificado. La fecha/hora se almacena en formato numérico (`time_t`).

- `notafter` (tipo SQL: int): La fecha en la que el certificado expira. La fecha/hora se almacena en formato numérico (`time_t`).

- `notifyto` (tipo SQL: char 65): Una dirección de correo electrónico a la que la RA enviará las notificaciones relacionadas con el certificado. Esta columna puede contener un valor nulo.

- `ea` (tipo SQL: char 65): El valor del componente (dirección de correo electrónico) del nombre distinguido del titular del certificado. Se almacena un valor nulo si este componente no está presente en el DN.

- `cn` (tipo SQL: char 65): El valor del componente CN (nombre común) del nombre distinguido del titular del certificado. Se almacena un valor nulo si este componente no está presente en el DN.

- `ou` (tipo SQL: char 65): El valor del componente OU (unidad organizativa) del nombre distinguido del titular del certificado. Se almacena un valor nulo si este componente no está presente en el DN. Si el DN contiene más de un componente OU solamente el primero se almacena en esta columna.

- `o` (tipo SQL: char 2): El valor del componente O (organización) del nombre distinguido del titular del certificado. Se almacena un valor nulo si este componente no está presente en el DN. Si el DN contiene más de un componente O solamente el primero se almacena en esta columna.

- `c` (tipo SQL: char 2): El valor del componente C (país) del nombre distinguido del titular del certificado. Se almacena un valor nulo si este componente no está presente en el DN.

- `sntext` (tipo SQL: char 65): El número de serie del certificado, en formato hexadecimal.

- `snint` (tipo SQL: int): El número de serie del certificado en formato decimal. Esta columna contiene un valor nulo si el número de serie precisa más de cuatro *bytes* para ser representado en formato binario.

- `batchid` (tipo SQL: char 65): Elemento identificador del lote que contiene la petición a partir de la que el certificado fue emitido. Si el certificado se generó procesando una petición individual realizada en KeyOne CA, entonces esta columna contiene el identificador del lote auxiliar generado por la CA.



- batchentry (tipo SQL: int): La posición que el certificado ocupa en el lote identificado por la columna batchid. La posición se indica como un entero decimal mayor o igual que cero.

- revreason (tipo SQL: int): El código de la razón de revocación. El código de la razón se almacena como un número decimal y sus posibles valores están definidos en [RFC2459]. Está columna contiene el valor nulo si el certificado no está revocado o suspendido.

- revdate (tipo SQL: int): La fecha de revocación del certificado. La fecha/hora se almacena en formato numérico (time_t). Está columna contiene el valor nulo si el certificado no está revocado o suspendido.

- p12present (tipo SQL: int): Esta columna contiene el valor 1 si (1) la CA emitió un PKCS #12 junto con el certificado, y (2) el PKCS #12 generado está disponible en la base de datos de la CA (en tabla de lotes). En cualquier otro caso, la columna contiene el valor nulo.

CRLs

Todas las CRLs que el sistema KeyOne genera son almacenadas en la tabla crl_ca de la base de datos de KeyOne CA. Esta tabla es utilizada por KeyOne CA para almacenar todas las CRLs que emite.

Las columnas de esta tabla son las siguientes:

- crltype (tipo SQL: int): Un número positivo que identifica la plantilla de CRL que se utilizó para generar la CRL. Con este propósito las plantillas de CRL que se definen en KeyOne CA son numeradas de forma secuencial, comenzando por el cero.

- thisupdate (tipo SQL: int): La fecha y la hora de emisión de la CRL. La fecha/hora se almacena en formato numérico (time_t).

- nextupdate (tipo SQL: int): La fecha y hora máxima en la que se emitirá próxima actualización de la CRL. La fecha/hora se almacena en formato numérico (time_t).

- crlnumber (tipo SQL: int): Si la CRL contenía la extensión id-ce-cRLNumber (definida en [X.509]), entonces esta columna contiene el valor de dicha extensión (un entero positivo en formato decimal). De otro modo, si la extensión no fue incluida en la CRL, esta columna contiene el valor nulo.

Registros de auditoría

Todos los eventos que se registran en el sistema KeyOne son almacenados en una tabla logs del componente en el que se produjo el evento.

Las columnas de esta tabla son las siguientes::

- timelog (tipo SQL: int): Fecha y hora en la que se produjo el evento. La fecha/hora se representa en formato numérico.

- author (tipo SQL: char 255): Nombre distinguido de la entidad que provocó el evento. Corresponde con el nombre distinguido del PSS que estaba en uso cuando se realizó la operación. El nombre distinguido se representa como una cadena de caracteres según el formato que se define en [RFC2253].

- `Role` (tipo SQL: char 65): Una cadena de caracteres que indica el tipo de entidad que provocó el evento. Corresponde al valor del atributo rol del PSS que estaba en uso cuando se realizó la operación.
- `evtype` (tipo SQL: int): Un número que indica el tipo del evento.
- `event` (tipo SQL: int): Un número que identifica unívocamente al evento dentro del conjunto de eventos del mismo tipo que son generados por el mismo módulo.
- Un número que identifica el módulo que generó el evento (columna `modu`). Esta columna contiene un valor nulo para los eventos del tipo MARCA.
- `Evlevel` (tipo SQL: int): Un número que indica la importancia del evento.
- `Obser` (tipo SQL: char 255): Una cadena de caracteres que describe el evento. Para algunos eventos, la descripción va seguida de una lista de parámetros (separados por caracteres de salto de línea) cuyo valor varía dependiendo de los datos sobre los que se realizó la operación.
- `Indlevel` (tipo SQL: int): Un número que indica el nivel de anidamiento del evento. Los eventos que producen algunas operaciones se organizan jerárquicamente de forma que un evento puede agrupar a otros de nivel inferior. Para los eventos del primer nivel, esta columna contendrá el valor 1, Para eventos de segundo nivel y superiores, el valor será mayor que 1. El valor 0 se almacenará para aquellos eventos en los que esta característica no sea aplicable

Para archivar los datos en la base de datos, se utiliza la API de base de datos i3D. Esta API es una interfaz Scryptor que toma la forma de un objeto de Scryptor (i3DHandler), que proporciona métodos para establecer asociaciones con tablas lógicas i3D, de forma que es posible añadir, modificar y consultar los registros lógicos escondiendo los detalles de la tecnología i3D de las tablas físicas subyacentes.

Esta API utiliza los servicios de una API C++ de acceso a base de datos que es funcionalmente equivalente (correspondencia uno a uno) con la API de acceso a base de datos en Scryptor.

Las operaciones SQL se pueden realizar sobre registros de las tablas lógicas y se ejecutan operaciones criptográficas para aplicar los mecanismos de seguridad i3Ds. Más adelante se describen las operaciones criptográficas que implica la realización de operaciones sobre las tablas lógicas.

Cada entrada incluye el tiempo en el que el evento se produjo. El servicio de archivado gestiona los siguientes elementos: certificados, CRLs y registros de auditoría. En todos los casos, el tiempo se incluye del siguiente modo:

- Para los certificados el campo `notBefore` contiene la hora en la que el certificado fue generado. El evento en este caso corresponde con la generación del certificado y, por lo tanto, la hora en la que el evento se produjo coincide con la hora en la que el certificado fue generado.
- Para las CRLs el campo `thisUpdate` contiene la hora en la que la CRL fue generada. El evento en este caso corresponde con la generación de la CRL y, por lo tanto, la hora en la que se produjo el evento coincide con la hora de generación de la CRL.



- Para registros de auditoría, la columna `timeLog` contiene la fecha y la hora en la que se produjo el evento.

Esta función está relacionado con el registro de la hora en los archivos. En este caso, esta funcionalidad está implicada en la realización de operaciones SQL asociadas a las funciones de gestión i3D.

El archivo de KeyOne no incluye parámetros seguridad críticos de manera desprotegida. En la base de datos de KeyOne no se guardan parámetros de seguridad críticos, sino que éstos se guardan siempre en el almacén privado seguro (PSS) que está asociado a la aplicación.

Una clave simétrica i3D se deriva de la contraseña del PSS según las especificaciones de [PKCS5], utilizando sal y un contador de iteraciones. Esta clave se utiliza para cifrar los parámetros de seguridad como atributos del PSS.

FAU_SAR.1.1

El sistema KeyOne proporciona a los usuarios que sean autenticados por la aplicación KeyOne (administradores de la autoridad de certificación, administradores de la autoridad de validación y administradores de la autoridad de sellado de tiempo) la capacidad de lectura de toda la información concerniente a los registros de auditoría (fecha y hora del evento, tipo del evento, identidad del sujeto, resultado del evento, rol de la identidad del sujeto, nivel del evento, categoría del evento, observaciones e identificador del evento) del registro de auditoría.

Como se indica en la función FIA_UAU.2.1, el sistema KeyOne requiere que los usuarios se autentiquen antes de permitirles cualquier acción. Este sistema de autenticación resulta en un control de acceso cuando los usuarios tratan de leer la información relativa a los registros de auditoría. Por lo tanto el control de acceso respecto a la lectura de la información de auditoría es el mecanismo de autenticación aplicado cuando los usuarios intentan acceder a la funcionalidad de KeyOne, tal y como se explica en la sección FIA_UAU.2.1.

La información que los usuarios autenticados pueden acceder son todos los datos relativos a los registros de auditoría. Esto se explica en las secciones Provisión de registros de auditoría en las aplicaciones KeyOne CA y KeyOne TSA y Provisión de registros de auditoría en la aplicación KeyOne VA.

FAU_SAR.1.2

El sistema KeyOne proporciona los registros de auditoría de una manera adecuada para que el usuario pueda interpretar la información.

Provisión de registros de auditoría en las aplicaciones KeyOne CA y KeyOne TSA

La función de consulta de registros de auditoría de estas aplicaciones está disponible mediante la opción `View logs` del menú `Miscellaneous`.

El propósito de esta funcionalidad es mostrar la lista de eventos que hayan sido registrado como resultado de las operaciones ejecutadas por el producto KeyOne. La información que se reporta en relación a los eventos es la siguiente:

- Información sobre los registros de eventos.



La siguiente información se muestra para cada evento:

- Icono[13]: Esta información aparece a la izquierda de cada fila e indica la categoría del evento. Los eventos se clasifican en las siguientes categorías según a su importancia: `Informativo` (`i`), `Marca` (`>`), `Advertencia`(`!`), `Error` (`!!`), `Error fatal` (`!!!`).
- Fecha: Fecha y hora en la que se produjo el evento. El formato es el siguiente: `YYYY-MM-DD HH-MM-SS`.
- Evento: Tipo e identificador del evento.
- Observaciones: Descripción textual sobre el evento.

- Información detallada sobre cada evento registrado.

  La siguiente información detallada se muestra para cada evento:

  - Categoría: Indica la importancia del evento. Los posibles valores de este campo son: `Informativo` (los eventos de esta categoría proporcionan información sobre las operaciones que se realizan con éxito), `Marca` (cuando comienza y finaliza una sesión administrativa), `Advertencia` (indica la detección de una condición anormal durante la realización de una operación, pero que no causó el fallo de la operación), `Error` (indica el fallo de una operación debido a un error predecible), `Error fatal` (indica que una circunstancia excepcional e impredecible ocurrió durante una operación).
  - Fecha: Fecha y hora en la que se produjo el evento.
  - Autor: Nombre distinguido de la entidad que generó el evento.
  - Rol: Tipo de la entidad que generó el evento. Los valores posibles de este campo son: `CA-admin` (Administrador de la Autoridad de certificación), `RA-Responsible` (Responsable de la Autoridad de registro) y `RA-Approver` (Aprobador de la autoridad de registro).
  - Tipo de evento: Los eventos se clasifican en los siguientes tipos: `MARCA` (Evento que pertenece a la categoría "Marca"), `CRYPTO` (evento criptográfico), `DB` (evento de base de datos), `ENGINE` (evento del motor), `HCI` (evento en la interfaz de usuario), `LIB` (evento de librería).
  - Id. del evento: Número que identifica unívocamente al evento entre el conjunto de eventos del mismo tipo que hayan sido generados por el mismo módulo.
  - Modulo: Identifica el módulo en el que se produce el evento. Los posibles módulos son: `CA`, `RA`, `Library: StoreServiceHandler`, `Library: SecureStore`, `Library:LocalStore`, `Library:Template`, `Library:Policies`, `TSA`.
  - Nivel: Un número que indica el nivel de anidamiento del evento. Los eventos que determinadas operaciones producen se organizan jerárquicamente de forma que un evento puede agrupar a otros eventos de segundo nivel,

[13] *Información disponible en la aplicación KeyOne CA.*



dependiendo de su dificultad. Para los eventos de primer nivel, este campo indica el valor 1. Para los niveles segundo y siguientes, este campo indica un valor mayor que 1. Para los eventos en los que esta característica no sea aplicable, se muestra el valor 0.

- Observaciones: Descripción textual de evento. Para algunos eventos, la descripción va seguida de una lista de parámetros cuyo valor varía dependiendo de los datos sobre los que se ejecute la operación. Algunos de los parámetros que se incluyen para el evento "generación de certificado" son: el número de serie y el nombre distinguido del titular del certificado emitido y la plantilla de certificación que se haya aplicado.

Provisión de registros de auditoría en la aplicación KeyOne VA

The audit records browsing function related to these applications is available from the `Browsing logs` option in the `Logs` menu.

La función de consulta de los registros de auditoría de esta aplicación está disponible desde la opción `Consulta de logs` del menú `Logs`.

El propósito de esta funcionalidad es mostrar la lista de eventos que se hayan registrado como resultado de las operaciones realizadas por el producto KeyOne VA. La información que se reporta en relación a estos eventos es la siguiente:

- Información de los registros de eventos.

  Para cada evento se muestra la siguiente información:

  - Categoría: Indica la categoría del registro. Los registros se clasifican en las siguientes categorías según su importancia: `Informativol`, `Marca`, `Advertencia`, `Error`, `Error fatal`.
  - Fecha: Fecha y hora en la que se produjo el evento. El formato es el siguiente: `YYYY-MM-DD HH-MM-SS`.
  - Módulo: Módulo que generó el evento.
  - Evento: Tipo e identificador del evento.
  - Observaciones: Descripción textual del evento.

- Información detallada de cada evento registrado.

  Para cada evento se muestra la siguiente información detallada:

  - Categoría: Indica la importancia del evento. Los posibles valores de este campo son: `Informativo` (los eventos de esta categoría proporcionan información sobre las operaciones que se realizan con éxito), `Marca` (cuando comienza y finaliza una sesión administrativa), `Advertencia` (indica la detección de una condición anormal durante la realización de una operación, pero que no causó el fallo de la operación), `Error` (indica el fallo de una operación debido a un error predecible), `Error fatal` (indica que una circunstancia excepcional e impredecible ocurrió durante una operación).
  - Fecha: Fecha y hora en la que se produjo el evento.



- Author: Identifica al autor del registro. Se pueden asignar los siguientes valores: nombre distinguido de la entidad que generó el evento, nombre distinguido de la entidad que causó el evento, identificador de la tarea que generó el evento, y en caso de eventos subordinados, identificador del evento padre.

- Rol: Tipo de entidad que generó el evento. Los valores posibles de este campo son: `VA-user` (usuario de la Autoridad de validación), `VA-job` (proceso de la Autoridad de validación), `VA-ocspResponder` (servidor de la Autoridad de validación).

- Tipo de evento: Los eventos se clasifican en los siguientes tipos: `MARCA` (Evento que pertenece a la categoría "Marca"), `CRYPTO` (evento criptográfico), `DB` (evento de base de datos), `ENGINE` (evento del motor), `HCI` (evento en la interfaz de usuario), `LIB` (evento de librería).

- Id. del evento: Número que identifica unívocamente al evento entre el conjunto de eventos del mismo tipo que hayan sido generados por el mismo módulo.

- Modulo: Identifica el módulo en el que se produce el evento. Los posibles módulos son: `OCSPRESPONDER`, `OCSPUPDATER`, `OCSPADMIN`, `LIB_STORESERVICE`, `LIB_SECURESTORE`, `LIB_LOCALSTORE`, `LIB_TEMPLATE`, y `LIB_POLICIES`.

- Level: A number indicating the event nesting level. Events produced by some operations are hierarchically organized so that an event may group other second-level events, depending on their difficulty. For first-level events, this field indicates a value of 1. For second and subsequent level event, this field indicates a value greater that 1. For events where the characteristic is not applicable, a value of 0 will be shown.

- Nivel: Un número que indica el nivel de anidamiento del evento. Los eventos que determinadas operaciones producen se organizan jerárquicamente de forma que un evento puede agrupar a otros eventos de segundo nivel, dependiendo de su dificultad. Para los eventos de primer nivel, este campo indica el valor 1. Para los niveles segundo y siguientes, este campo indica un valor mayor que 1. Para los eventos en los que esta característica no sea aplicable, se muestra el valor 0.

- Observaciones: Descripción textual de evento. Para algunos eventos, la descripción va seguida de una lista de parámetros cuyo valor varía dependiendo de los datos sobre los que se ejecute la operación. Algunos de los parámetros que se incluyen para el evento "generación de certificado" son: el número de serie y el nombre distinguido del titular del certificado emitido y la plantilla de certificación que se haya aplicado.

- Mostrar registros subordinados: Aparece cuando se visualiza un registro de primer nivel, pulsar este botón para ver los eventos de segundo nivel que se derivan de este evento.

- Mostrar evento padre: Aparece cuando se visualiza un evento de nivel 2, pulsar este botón para ver el primer nivel del cual este evento depende.



FAU_SAR.3.1

El sistema KeyOne proporciona la capacidad de realizar búsquedas, clasificar y ordenar las siguientes información de las bases de datos de auditoría.

- Fecha y hora del evento.
- Tipo del evento.
- Identidad del usuario.
- Rol del usuario.
- Identificador del evento.
- Módulo que generó el evento.
- Categoría del evento (importancia del evento).
- Observaciones sobre el evento].

Esta función es aplicable a los componentes KeyOne VA, KeyOne CA y KeyOne TSA. Las secciones `Screen for browsing logs in KeyOne CA and KeyOne TSA applications` y `Screen for browsing logs in KeyOne VA application` del capítulo `Security Audit` del documento [FUNCSPEC], especifican todos los detalles sobre las operaciones de búsqueda, ordenación y clasificación aplicables a la información de auditoría.

FAU_STG.1.1

El sistema KeyOne protege del borrado los registros de auditoría que se almacenan.

The unauthorized deletion of audit records can take place from KeyOne applications or from a component that is outside of the KeyOne system (like a database client).

El borrado no autorizado de registros de auditoría puede ocurrir desde las aplicaciones KeyOne o desde un componente que está fuera del sistema KeyOne (como un cliente de la base de datos)

- Borrado no autorizado desde una aplicación KeyOne

  Las aplicaciones KeyOne **no proporcionan funcionalidad que permita el borrado explícito de los registros de auditoría que están almacenados**, y además la aplicación almacena la contraseña de la base de datos de forma segura para evitar los borrados no autorizados. La contraseña de la base de datos se almacena cifrada de forma segura por el administrador. El cifrado de esta contraseña se realiza durante el proceso de configuración de la base de datos. La funcionalidad que permite configurar la conexión con la base de datos en los productos KeyOne es la responsable de cifrar la contraseña de base de datos y de almacenarla en el almacén privado seguro de la aplicación.

- Borrado no autorizado desde un componente que no forma parte de KeyOne

  Puesto que la contraseña de la base de datos se almacena de forma segura en el almacén privado seguro de la aplicación, no es posible para un componente externo obtener esta contraseña y acceder a la base de datos de la aplicación. Adicionalmente, el apéndice CPS de KeyOne 2.1 describe un **mecanismo de**

control de acceso a las bases de datos de la aplicación que protege el acceso a la base de datos.

FAU_STG.1.2_1

El sistema KeyOne es capaz de detectar modificaciones no autorizadas de los registros de auditoría.

La base de datos en la que se almacenan los registros es una base de datos i3D y consecuentemente proporciona el Sistema de Integridad de Bases de datos; este sistema asegura la integridad de todos los datos que se almacenan en la base de datos de las aplicaciones. Los registros de auditoría son parte de la base de datos KeyOne y, por tanto, este sistema proporciona también el servicio de integridad a los registros de auditoría.

La integridad de una base de datos i3D puede verificarse con la herramienta de línea de comandos `i3dverify.ws` que se proporciona con los productos KeyOne. Esta herramienta realiza las verificaciones utilizando algunos certificados y claves según sea el tipo de comprobación que se lleva a cabo. Este *script* debe ejecutarse utilizando un intérprete de comandos del sistema operativo, desde la carpeta `scripts` de la carpeta de instalación del producto.

FAU_STG.1.2_2

El sistema KeyOne es capaz de evitar modificaciones no autorizadas de los registros de auditoría, puesto que la tecnología KeyOne impide re-escribir los registros de auditoría (los registros de auditoría no se re-escriben automáticamente).

Puesto que los registros de auditoría están almacenados en una base de datos de i3D, el sistema de registro de KeyOne garantiza que los registros de auditoría no se sobre escriban nunca.

La API de bases de datos i3D es una interfaz en Scryptor para acceder a bases de datos i3D. Esta API toma la forma de un objeto de Scryptor (`i3DHandler)` el cual proporciona los métodos para establecer asociaciones con tablas lógicas i3D, de manera que sea posible añadir, actualizar y consultar los registros lógicos ocultando los detalles de la tecnología i3D de las tablas físicas subyacentes.

Once an i3D session has been started, it is said that the session is active. This means that the user may perform SQL operations over the logical table records, and the performed operations will be associated to that session. How these operations over the logical table affect the historic record table and the browsing table is described below.

Una ve que comienza una sesión i3D, se dice que la sesión está activa. Esto significa que el usuario puede realizar operaciones SQL sobre los registros de la tabla lógicas y que las operaciones que se realicen son asociadas a esta sesión. A continuación se explica cómo afectan a la tabla de históricos y la tabla de consultas las operaciones realizadas sobre la tabla lógica

- Inserción de un registro lógico

  Causa la inserción de un registro en la tabla de registros históricos (registro histórico) que contiene los datos que hay que almacenar codificados en DER (columna `info`) y otras columnas de control. El nuevo registro incluye



información sobre el identificador de la sesión activa (columna `sessionid`). El registro completa se firma simétricamente utilizando la clave de sesión (columna `hmac`).

Además, se añade en la tabla de consultas un registro que está asociado al registro histórico, (a través de la columna `hmac`). Este registro contiene en columnas no codificadas parte de los datos del registro lógico que se almacena (el número y el tipo de las columnas depende de la definición de la tabla lógica).

- Actualización de un registro lógico

  Causa la inserción de un registro histórico que contiene los nuevos datos del registro lógico y que está relacionado con el registro histórico previo del mismo registro lógico.

  El nuevo registro incluye información sobre el identificador de la sesión activa (columna `sidcurrent`). El registro completo se firma simétricamente utilizando la clave de sesión (columna `hmac`).

  El registro de la tabla de consulta asociado al registro histórico anterior se actualiza con los nuevos datos y se asocia con el nuevo registro histórico (a través de la columna `hmac`).

- Selección y recuperación de un registro lógico.

  Las consultas SQL de selección que el usuario solicita se ejecutan sobre la tabla de consultas. Cada registro de esta tabla corresponde a un registro lógico.

  Una vez que el registro deseado ha sido seleccionado de la tabla de consultas, se accede a la tabla de registros históricos (a través del valor de la columna `hmac`) para obtener el último registro histórico asociado al registro lógico. El valor actual del registro lógico se obtiene decodificando los datos almacenados en la columna `info` del registro histórico.

  Esta operación no causa ni la inserción ni la modificación de los datos de ninguna tabla.

- Borrado de un registro lógico

  Causa la inserción de un registro histórico marcado de una manera especial para indicar que se borra el registro lógico y que, por lo tanto, no se van a asociar más registros históricos al mismo (columna `deleted`). El nuevo registro histórico incluye información sobre el identificador de la sesión activa (columna `sidcurrent`). El registro complete se firma simétricamente utilizando la clave de sesión (columna `hmac`).

  Adicionalmente, también se borra de la tabla de consultas la entrada correspondiente al registro lógico que se esté borrando, de forma que sólo quede rastro de su existencia en la tabla de registros históricos.

Los registros de auditoría se almacenan en una tabla de logs en la base de datos i3D. El mecanismo de registro de los eventos siempre implica operaciones de inserción de registros lógicos y nunca operaciones de actualización o borrado de registros lógicos. En consecuencia, la funcionalidad que registra los registros de auditoría está relacionada con la función que inserta registros lógicos en la base de datos i3D.

FCS – Soporte criptográfico

FCS_CKM.1.1_1

El sistema KeyOne genera claves criptográficas de acuerdo con los algoritmos simétricos 3DES (FIPS 46-3, Data Encryption Standard) y RC4, utilizando los siguientes tamaños de clave:

- Algoritmo de generación de claves 3DES: Claves de 168 bits de tamaño.
- Algoritmo de generación de claves RC4: Claves de 128 bits de tamaño.

La generación de un algoritmo criptográfico tiene lugar en los siguientes procesos: Proceso de generación de un almacén privado seguro, servicios relacionados con la tecnología i3D, y generación de una comunicación SSL/TLS entre componentes de KeyOne.

Proceso de generación de un almacén privado seguro

El almacén privado seguro (PSS) es un objeto seguro en el que se pueden almacenar datos sensibles que deben protegerse frente al acceso o la modificación ilícita (claves privadas, certificados, datos de configuración, etc). La implementación del PSS puede hacerse en medios: disco, tarjeta *smartcard* o dispositivo criptográfico.

Para acceder al PSS se requiere una contraseña. De la contraseña se deriva una clave utilizando "sal" y un contador de iteraciones según las recomendaciones PKCS#5. El esquema de cifrado subyacente utiliza una clave simétrica 3DES de 192 bits. Esta clave se utiliza para los siguientes propósitos:

- Confidencialidad: Los datos del PSS se cifran utilizando una clave 3DES.
- Integridad: El PSS[14] entero se firma calculando el resumen SHA-1 *hash* de los datos y cifrando el resultado con una clave 3DES. Un resumen SHA1 se calcula sobre el campo `tobeSigned` de los certificados[15] firmados.

La funcionalidad relativa a la generación de un almacén privado seguro invoca a una función que genera la clave simétrica 3DES.

Servicios relacionados con la tecnología i3D

i3D technology is based on the use of digital signatures and other cryptographic techniques in order to assure database integrity and non-repudiation. In the cryptographic processes related to the i3D technology the generation of symmetric cryptographic keys (192 bits 3DES) takes place.

La tecnología i3D se basa en el uso de firmas digitales y otras técnicas criptográficas para asegurar la integridad de la base de datos y el no repudio. En los procesos criptográficos relacionados con la tecnología i3D, tiene lugar la generación de claves criptográficas (3DES de 192 bits).

---

[14] *Excepto para objetos firmados, tales como certificados o CRLs.*
[15] *Certificados o CRLs.*



Los procesos i3D relacionados con la generación de claves criptográficas simétricas son los siguientes:

- Cada vez que un usuario comienza una sesión[16] i3D con una tabla lógica se añaden dos registros a la tabla de sesión: la entrada de inicio de sesión y la entrada de final de sesión. Estos registros contienen varias columnas de control entre los cuales se incluye el identificador de sesión (columna `sessionid`). Este identificador es diferente para todas las sesiones i3D que inician los diferentes usuarios sobre la tabla lógica. Cuando comienza una sesión i3D, se genera una clave simétrica aleatoria 3DES de 192 bits. Recibe el nombre de clave de sesión.

- Esta clave i3D se almacena en el registro de inicio de sesión y se cifra asimétricamente con destino a los *masters* de la base de datos, de forma que sólo los *masters* puedan conocerla. El cifrado asimétrico implica la generación de la clave criptográfica simétrica 3DES relacionada con el sobre digital.

La funcionalidad de arranque y parada de los servidores KeyOne es responsable de invocar la funcionalidad relativa a la gestión i3D. La gestión i3D implica la funcionalidad de generación de claves simétricas

Generación de una comunicación SSL/TLS entre componentes KeyOne

Varias de las comunicaciones entre distintos componentes de KeyOne y los servidores implican el establecimiento de una comunicación SSL/TLS. Cada establecimiento de un canal SSL/TLS implica la generación de una clave simétrica (clave de sesión). El algoritmo que se utiliza para generar la clave simétrica es negociada entre el cliente SSL/TLS y el servidor SSL/TLS. Los servidores SSL/TLS pueden ser configurados para especificar los algoritmos que aceptarán en el proceso de negociación de los parámetros SSL/TLS. Por defecto, estos servidores se configuran para aceptar los siguientes valores para los algoritmos SSL/TLS:

- RC4 como algoritmo simétrico, SHA como algoritmo de hash, y RSA como algoritmo asimétrico.

- RC4 como algoritmo simétrico, MD5 como algoritmo de hash, y RSA como algoritmo asimétrico.

- 3DES como algoritmo simétrico, SHA como algoritmo de hash, y RSA como algoritmo asimétrico.

En consecuencia, en la comunicación SSL/TLS entre componentes KeyOne se utilizan, por defecto, los algoritmos simétricos RC4 y 3DES. Los servidores SSL/TLS KeyOne pueden ser configurados para aceptar otros algoritmos criptográficos.

La función de generación de claves simétricas es invocada desde los siguientes procesos:

- Comunicación SSL/TLS entre navegadores de Internet y servidores KeyOne

- Comunicación SSL/TLS entre KeyOne LRA y KeyOne CA

---

[16] *Las operaciones están agrupadas en sesiones (sesiones i3D), y entonces para consultar o realizar cambios en una tabla el usuario debe primero abrir una sesión con esta tabla.*

- Comunicación SSL/TLS entre los servidores *online* de KeyOne y los administradores

- Comunicación SSL/TLS entre KeyOne VA y el servidor KeyOne CertStatus

Comunicación SSL/TLS entre navegadores de Internet y servidores KeyOne

Las aplicaciones KeyOne constan de un servidor KeyOne y de un componente de cliente *web* que ofrece la funcionalidad del producto. La comunicación entre el servidor KeyOne y el cliente *web* es una comunicación SSL/TLS (HTTPS local). La comunicación SSL/TLS se inicia cuando el administrador del producto arranca el servidor KeyOne.

Los algoritmos utilizados son distintos dependiendo de las aplicaciones KeyOne:

- Aplicación KeyOne

  Este componente utiliza el protocolo SSL 3.0 para que el servidor KeyOne se comunique con el componente del cliente *web*. Por defecto, los algoritmos que el servidor KeyOne (servidor SSL) acepta son los siguientes:

  - RC4 (40 bits) como algoritmo simétrico, MD5 como algoritmo de *hash*, y RSA como algoritmo asimétrico.

  - RC2 (40 bits) como algoritmo simétrico, MD5 como algoritmo de *hash*, y RSA como algoritmo asimétrico.

  - DES como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.

  - DES (40) como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.

  - RC4 (128 bits) como algoritmo simétrico, MD5 como algoritmo de *hash*, y RSA como algoritmo asimétrico.

  - RC4 (128 bits) como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.

  - 3DES como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.

  La configuración SSL se encuentra en el fichero de configuración `config_ca_ssl_connection_callbaks.ws`[17].

  Normalmente no conviene utilizar los algoritmos RC4 (40 bits), RC2 (40 bits), DES (40) y DES (56), puesto que son criptográficamente débiles. Por lo tanto, se recomienda configurar el sistema para que utilice criptografía fuerte. Este requerimiento se puede conseguir mediante dos alternativas:

    - Cambiando el fichero de configuración SSL para restringir los algoritmos a utilizar con SSL. EL apéndice CPS de KeyOne 2.1 contiene el procedimiento que seguir para cumplir este requisito.

---

[17] *Este campo está ubicado en la carpeta* `config` *del directorio de instalación de KeyOne CA.*



- Configurando el componente de cliente *web* (cliente SSL) para que solo utilice criptografía fuerte. El apéndice CPS de KeyOne 2.1 incluye un como requisito la utilización de criptografía fuerte por parte de los clientes *web*.

- Aplicación KeyOne LRA

  Este componente utiliza el protocolo SSL 3.0 para la comunicación entre el servidor KeyOne y el componente de cliente *web*. Por defecto, los algoritmos criptográficos que el servidor KeyOne (servidor SSL) acepta son los siguientes:

  - RC4 (40 bits) como algoritmo simétrico, MD5 como algoritmo de *hash*, y RSA como algoritmo asimétrico.
  - RC2 (40 bits) como algoritmo simétrico, MD5 como algoritmo de *hash*, y RSA como algoritmo asimétrico.
  - DES como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.
  - DES (40) como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.
  - RC4 (128 bits) como algoritmo simétrico, MD5 como algoritmo de *hash*, y RSA como algoritmo asimétrico.
  - RC4 (128 bits) como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.
  - 3DES como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.
    - Since RC4 (40 bits), RC2 (40 bits), DES (40) and DES (56) algorithms are soft cryptography, they are not normally suitable to be used. Therefore it is recommended to configure the system for hard cryptography use. This requirement can be accomplished configuring the web client component (SSL client) in order to only use hard cryptography. The appendix CPS de KeyOne 2.1 includes a requirement in order to use web clients with hard cryptography.
    - Normalmente no conviene utilizar los algoritmos RC4 (40 bits), RC2 (40 bits), DES (40) y DES (56), puesto que son criptográficamente débiles. Por lo tanto, se recomienda configurar el sistema para que utilice criptografía fuerte. Este requerimiento se puede conseguir configurando el componente de cliente *web* (cliente SSL) para que solo utilice criptografía fuerte. El apéndice CPS de KeyOne 2.1 incluye un como requisito la utilización de criptografía fuerte por parte de los clientes *web*.

- Aplicación TSA.

  Este componente puede utilizar el protocolo SSL 3.0 o SSL 3.1 (TLS) para la comunicación entre el servidor KeyOne y un cliente *web*. Por defecto, los algoritmos criptográficos que acepta el servidor KeyOne (servidor SSL) son los siguientes:

- RC4 (128 bits) como algoritmo simétrico, MD5 como algoritmo de *hash*, y RSA como algoritmo asimétrico.
- RC4 (128 bits) como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.
- 3DES como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.

La configuración SSL/TLS se encuentra en el fichero de configuración `config_tsa_server_server.ws`[18].

La comunicación SSL/TLS arranca cuando el administrador inicia el servidor KeyOne.

Comunicación SSL/TLS entre KeyOne LRA y KeyOne CA

Cada vez que el producto LRA arranca, se conecta con el servidor online de KeyOne CA y le envía un lote UR[19]. Por su parte, el servidor incluye en el lote de respuesta los *scripts* que implementan la aplicación de administración de KeyOne LRA (*scripts* descargables). Estos *scripts* serán incluidos en los parámetros del lote de respuesta utilizando un formato comprimido.

Esta comunicación consiste en una conexión SSL/TLS con autenticación de cliente. Para comunicarse de acuerdo a este protocolo, es necesario que un certificado de cliente SSL esté instalado en el almacén privado seguro de KeyOne LRA y que un certificado de servidor SSL esté instalado en el servidor *online* de KeyOne. KeyOne LRA utiliza el mismo certificado para comunicarse de acuerdo al protocolo SSL y para firmar digitalmente cada petición (lote) que envía al servidor *online*.

La comunicación entre KeyOne LRA y KeyOne CA comienza cuando se envían los *scripts* descargables a KeyOne LRA y se mantendrá durante la operación de la Autoridad de registro

Adicionalmente, la comunicación entre KeyOne LRA y la base de datos de KeyOne CA se lleva a cabo mediante una comunicación SSL/TLS entre KeyOne LRA y un servidor que reside en el componente KeyOne CA (servidor de consultas).

Los algoritmos que se utilizan son distintos dependiendo de la comunicación KeyOne:

- Comunicación entre KeyOne LRA y el servidor de consultas en el componente *online* de KeyOne CA.

  Esta comunicación utiliza el protocolo SSL 3.0/SSL3.1 (TLS). Por defecto, los algoritmos criptográficos que acepta el servidor KeyOne son los siguientes:

  - RC4 (128 bits) como algoritmo simétrico, MD5 como algoritmo de hash, y RSA como algoritmo asimétrico.
  - RC4 (128 bits) como algoritmo simétrico, SHA como algoritmo de hash, y RSA como algoritmo asimétrico.
  - 3DES como algoritmo simétrico, SHA como algoritmo de hash, y RSA como algoritmo asimétrico.

---

[18] *Este fichero está ubicado en el directorio* `config` *del directorio de instalación de KeyOne TSA.*
[19] *Lote de actualización.*



La configuración SSL/TLS se encuentra en el fichero de configuración `config_ca_online_browsing_server.ws`[20].

- Comunicación entre KeyOne LRA y el componente *online* de KeyOne CA.

  Esta comunicación utiliza el protocolo SSL 3.0/SSL3.1 (TLS). Por defecto, los algoritmos criptográficos que acepta el servidor KeyOne son los siguientes:

  - RC4 (128 bits) como algoritmo simétrico, MD5 como algoritmo de hash, y RSA como algoritmo asimétrico.
  - RC4 (128 bits) como algoritmo simétrico, SHA como algoritmo de hash, y RSA como algoritmo asimétrico.
  - 3DES como algoritmo simétrico, SHA como algoritmo de hash, y RSA como algoritmo asimétrico.

  La configuración SSL/TLS se encuentra en el fichero de configuración `config_ca_online_server.ws`[21].

La sección `Configuration interface for the SSL/TLS parameters` del capítulo `Cryptographic Support` en el documento [FUNCSPEC], describe la interfaz para la configuración de los parámetros SSL/TLS.

The SSL/TLS communication is started when the registration operator starts the KeyOne LRA server.

La comunicación SSL/TLS arranca cuando el operador de registro inicia KeyOne LRA.

Comunicación SSL/TLS entre los servidores *online* de KeyOne y los administradores *online*

La administración *online* soporta la pausa de un servidor online para realizar diversas tareas de mantenimiento, como la obtención de una copia de seguridad de la base de datos o la modificación de la configuración del servidor. Los servidores *online* de KeyOne (KeyOne CA online, KeyOne TSA y KeyOne CertStatus) disponen -sin necesidad de ser parados- de la capacidad de suspender el servicio desde las páginas de gestión del servidor.

When the service of an online server is paused, the server closes all connections with the database and does not attend the client's normal requests. The online administrator will then perform the maintenance tasks that caused the service to pause (backup, configuration reload) and, finally, it will restore it.

Cuando se suspende el servicio de un servidor *online*, el servidor cierra todas las conexiones con la base de datos y deja de atender las peticiones normales de los clientes. Entonces, el administrador *online* realiza las tareas de mantenimiento que provocaron la suspensión del servicio (copia de seguridad, recarga de la configuración) y, finalmente, lo restablece.

---

[20] *Este fichero está ubicado en la carpeta* `config` *folder del directorio de instalación de KeyOne TSA.*

[21] *Este fichero está ubicado en la carpeta* `config` *folder del directorio de instalación de KeyOne TSA.*

La conexión con el servidor de administración *online* es una conexión SSL/TLS con autenticación de cliente.

La comunicación entre el administrador *online* y el servidor KeyOne utiliza el protocolo SSL 3.0/SSL3.1 (TLS). Por defecto, lo algoritmos criptográficos que el servidor de KeyOne (servidor SSL) acepta son los siguientes:

- RC4 (128 bits) for the symmetric algorithm, MD5 for the hash algorithm, and RSA for the asymmetric algorithm.
- RC4 (128 bits) como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.
- 3DES como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.

La configuración SSL/TLS se encuentra en el fichero de configuración `config_online_administration_server.ws` de cada producto KeyOne.

La sección `Configuration interface for the SSL/TLS parameters` del capítulo `Cryptographic Support` del documento [FUNCSPEC], describe la interfaz de configuración de los parámetros SSL/TLS.

La sección `Interface for connecting to the online management service` del capítulo `Cryptographic Support` del documento [FUNCSPEC], describe la función para conexión con el servicio de gestión *online*.

Comunicación SSL/TLS entre KeyOne VA y el servidor KeyOne CertStatus

La comunicación entre KeyOne VA y el servidor KeyOne CertStatus se hace mediante SSL con autenticación de cliente. Cuando la VA necesita conocer el estado de los certificados, se comunica con el servidor CertStatus para pedirle que actualice la información sobre estado de revocación. Tanto las peticiones de la VA como las respuesta que emite el servidor CertStatus son firmadas. La lista de las VAs a las que el servidor de información de estados de certificados dará servicio, debe ser configurada.

Esta comunicación entre KeyOne VA y el servidor KeyOne CertStatus utiliza el protocolo SSL 3.0/SSL3.1 (TLS). Por defecto, lo algoritmos criptográficos que el servidor de KeyOne (servidor SSL) acepta son los siguientes:

- RC4 (128 bits) for the symmetric algorithm, MD5 for the hash algorithm, and RSA for the asymmetric algorithm.
- RC4 (128 bits) como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.
- 3DES como algoritmo simétrico, SHA como algoritmo de *hash*, y RSA como algoritmo asimétrico.

La sección `Configuring recognized VAs interface` del capítulo `Cryptographic Support` del documento [FUNCSPEC], describe la función para configurar VAs reconocidas.



La sección Configuration interface for the SSL/TLS parameters del capítulo Cryptographic Support del documento [FUNCSPEC], describe la interfaz de configuración de los parámetros SSL/TLS.

FCS_CKM.2.1

El sistema KeyOne distribuye claves criptográficas según los siguientes métodos de distribución de claves criptográficas:

- X509v3: ITU-T Recommendation X.509 | ISO/IEC International Standard 9594-8, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework.
- LDAPv2: RFC 1777 – Lightweight Directory Access Protocol.
- Mecanismos *offline*, descritos en el apéndice CPS de KeyOne 2.1.

Esta función se aplica a las claves criptográficas asimétricas. Con respecto a las claves criptográficas simétricas, éstas se almacenan de forma segura y no se distribuyen

- No se distribuye la clave simétrica 3DES del PSS.
- No se distribuyen las claves de sesión i3D.
- Las claves de sesión que se generan en las comunicaciones SSL/TLS, son claves temporales que sólo se distribuyen en el contexto[22] SSL/TLS.

La integridad y autenticidad de la clave pública y de cualesquiera parámetros asociados se mantiene durante la distribución inicial y las siguientes.

Los certificados raíz, puesto que son certificados firmados, deben obtenerse mediante mecanismos fiables. Como se describe en el apéndice CPS de KeyOne 2.1, estos mecanismos se basan en procedimientos *offline*, y aseguran la integridad y la autenticidad de la clave pública y de cualesquiera parámetros asociados durante la distribución inicial y las siguientes.

Para certificados no raíz, se pueden utilizar los certificados X.509v3 o los mecanismos LDAPv2. Aunque el protocolo LDAP se utilice para distribuir los certificados X.509, por lo que respecta a la publicación de la clave pública ésta se realiza mediante el certificado X.509 que la contiene, y por lo tanto, siempre se usan los certificados X.509 en la distribución y adicionalmente también LDAP.

Un certificado no raíz es una estructura firmada por un tercero de confianza (Autoridad de certificación) y, por tanto, en la que está garantizada la integridad y autenticidad de los datos que contiene (clave pública) .

Para los certificados DSA, los parámetros de las claves asociadas se pueden almacenar en las siguientes estructuras:

- Private Secure Store (PSS). All the data stored in the PSS are protected with integrity and authenticity security services, as described in the Cryptographic

---

[22] *Estas están cifradas asimétricamente con el certificado de servidor SSL/TLS server.*

`operations over the private secure store` section of the `Cryptographic Support` chapter in the [FUNCSPEC] document.

- Almacén privado seguro (PSS). Todos los datos que se almacenan en el PSS se protegen con servicios de seguridad sobre la integridad y la autenticidad, como se describe en la sección `Cryptographic operations over the private secure store` del capítulo `Cryptographic Support` del documento [FUNCSPEC]

- X.509 Certificates. El estándar [X509] define una estructura firmada en la que se aplican servicios de seguridad sobre la integridad y autenticidad.

Propiedades de los certificados auto-firmados

Un certificado auto-firmado generado por KeyOne CA tiene las siguientes propiedades:

- Se puede verificar la firma del certificado utilizando los datos que se proporcionan dentro del propio certificado;

- Los campos titular y emisor del certificado son idénticos.

La función de generación de certificados de CA raíz genera un certificado X.509 utilizando la especificación que se incluye en el documento [X509]. Puesto que esta especificación incluye todos los datos necesarios para verificar la firma que se incluye en el certificado, esta función utiliza los siguientes campos en el proceso de verificación:

- Campo `SignatureAlgorithm`: Contiene el identificador del algoritmo criptográfico que utilizó la CA para firmar el certificado. Este campo contiene un identificador de algoritmo que se utiliza para identificar un algoritmo criptográfico y los parámetros opcionales que están relacionados con el algoritmo. En la tecnología KeyOne es obligatorio incluir dentro de los certificados raíz que se firman con claves DSA, los parámetros de dichas claves DSA, no siendo posible recuperarlos mediante jerarquías o cualquier otro mecanismo (tal y como el estándar DSA especifica).

- Campo `Signaturevalue`: Este campo contiene una firma digital calculada sobre la codificación ASN.1 DER del `tbsCertificate` (*to be signed*)

Por lo tanto, la tecnología KeyOne requiere que un certificado raíz contenga dentro de él toda la información necesaria para verificar su firma.

La función de generación de certificados de CA raíz siempre genera certificados X.509 en los que los campos titular y emisor tienen el mismo valor.

La herramienta de comandos `createpss.ws` genera un almacén privado seguro, y las claves necesarias, CSRs y certificados, a partir de un fichero de propiedades dónde se indican las características de estas calves y certificados.

Para cada componente y servidor, un fichero de propiedades especifica las características de las claves y certificados para la entidad relacionada. Este fichero será utilizado como entrada del *script* que generará las claves y los certificados.

- KeyOne CA



El fichero *<type of entity>*_ca_properties.txt[23] indica las propiedades de las claves y los certificados. La variable *<type of key>*_keyAlgorithm[24] especifica el algoritmo de las claves. Por defecto, este algoritmo es RSA (valor rsaEncryption). Es posible cambiar este valor para generar claves DSA (en este caso el valor de la variable debe ser id_dsa). Si se indica claves DSA, es posible incluir los parámetros asociados en *<type of key>*_keyParameters[25] (si no se indican parámetros, la aplicación los generará de forma aleatoria). La variable *<type of key>*_isroot[26] indica si el certificado generado será raíz (valor 1) o no (valor 0). La variable subject indica el campo titular del certificado X.509 que será generado. Si la variable *<type of key>*_isroot vale 1, la aplicación asignará el valor de la variable subject al campo emisor del certificado.

El fichero db_master_properties.txt[27] indica las propiedades de las claves y los certificados de una entidad *master* i3D, en el caso de que tenga un PSS distinto al del componente CA. La variable *<type of key>*_keyAlgorithm[28] especifica el algoritmo de la clave. Por defecto, este algoritmo es RSA (valor rsaEncryption). Es posible cambiar este valor para generar claves DSA (en este caso el valor de la variable debe ser id_dsa). Si se indica claves DSA, es posible incluir los parámetros asociados en *<type of key>*_keyParameters [29] (si no se indican parámetros, la aplicación los generará de forma aleatoria). La variable *<type of key>*_isroot [30] indica si el certificado generado será raíz (valor 1) o no (valor 0). La variable subject indica el campo titular del certificado X.509 que será generado. Si la variable *<type of key>*_isroot vale 1, la aplicación asignará el valor de la variable subject al campo emisor del certificado.

En el caso de que las claves de master i3D fueran las de la CA, como se indica en el apéndice CPS de KeyOne 2.1, entonces no se utilizará este fichero, y las claves i3D serán generadas y mantenidas en el HSM.

- KeyOne LRA

---

[23] <type of entity> *indica el tipo de entidad que posee las claves y certificados (root_ca corresponde a la Autoridad de Certificación raíz, "root_online" corresponde a la Autoridad de Certificación online raíz, subord_ca corresponde a la Autoridad de Certificación subordinada, y subord_online corresponde a la Autoridad de Certificación online subordinada). Este fichero está ubicado en la carpeta scripts en la ruta de instalación del producto.*

[24] *Donde* <type of key> *indica el tipo de clave: csrs para claves de firma de certificados y CRL, ds para certificados de firma digital, de para cifrado de datos, ssl_local para SSL local y ssl_online para SSL.*

[25] *Donde* <type of key> *indica el tipo de clave: csrs para claves de firma de certificados y CRL, ds para certificados de firma digital, de para cifrado de datos, ssl_local para SSL local y ssl_online para SSL.*

[26] *Donde* <type of key> *indica el tipo de clave: csrs para claves de firma de certificados y CRL, ds para certificados de firma digital, de para cifrado de datos, ssl_local para SSL local y ssl_online para SSL.*

[27] *Este fichero está ubicado en la carpeta scripts de la ruta de instalación del producto.*

[28] *Donde* <type of key> *indica el tipo de clave: ds para certificados de firma digital y de para cifrado de datos.*

[29] *Donde* <type of key> *indica el tipo de clave: csrs para claves de firma de certificados y CRLs, ds para certificados de firma digital, de para cifrado de datos, ssl_local para SSL local y ssl_online para SSL.*

[30] *Donde* <type of key> *indica el tipo de clave: csrs para claves de firma de certificados y CRLs, ds para certificados de firma digital, de para cifrado de datos, ssl_local para SSL local y ssl_online para SSL.*

El fichero `lra_properties.txt`[31] indica las propiedades de las claves y los certificados. La variable *<type of key>*`_keyAlgorithm`[32] especifica el algoritmo de la clave. Por defecto, este algoritmo es RSA (valor `rsaEncryption`). La variable *<type of key>*`_isroot`[33] indica si el certificado generado será raíz (valor 1) o no (valor 0). La variable `subject` indica el campo titular del certificado X.509 que será generado. Si la variable *<type of key>*`_isroot` vale 1, la aplicación asignará el valor de la variable `subject` al campo emisor del certificado.

- KeyOne TSA

El fichero `tsa_properties.txt`[34] indica las propiedades de las claves y los certificados. La variable *<type of key>*`_keyAlgorithm`[35] especifica el algoritmo de las claves. Por defecto, este algoritmo es RSA (valor `rsaEncryption`). Es posible cambiar este valor para generar claves **DSA** (en este caso el valor de la variable debe ser `id_dsa)`. Si se indica claves DSA, es posible incluir los parámetros asociados en *<type of key>*`_keyParameters`[36] (si no se indican parámetros, la aplicación los generará de forma aleatoria). La variable *<type of key>*`_isroot`[37] indica si el certificado generado será raíz (valor 1) o no (valor 0). La variable `subject` indica el campo titular del certificado X.509 que será generado. Si la variable *<type of key>*`_isroot` vale 1, la aplicación asignará el valor de la variable `subject` al campo emisor del certificado.

El fichero `db_master_properties.txt`[38] indica las propiedades de las claves y los certificados de una entidad *master* i3D, en el caso de que tenga un PSS distinto al del componente TSA. La variable *<type of key>*`_keyAlgorithm`[39] especifica el algoritmo de la clave. Por defecto, este algoritmo es RSA (valor `rsaEncryption`). Es posible cambiar este valor para generar claves DSA (en este caso el valor de la variable debe ser `id_dsa)`. Si se indica claves DSA, es posible incluir los parámetros asociados en *<type of key>*`_keyParameters`[40] (si no se indican parámetros, la aplicación los generará de forma aleatoria). La variable

[31] *Este fichero está ubicado en la carpeta scripts en la ruta de instalación del producto.*
[32] *Donde* `<type of key>` *indica el tipo de clave:* `ds` *para certificados de firma digital y* `de` *para certificados de cifrado de datos.*
[33] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*
[34] *Este fichero está ubicado en la carpeta scripts de la ruta de instalación del producto.*
[35] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*
[36] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*
[37] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*
[38] *Este fichero está ubicado en la carpeta* `scripts` *de la ruta de instalación del producto.*
[39] *Donde* `<type of key>` *indica el tipo de clave:* `ds` *para certificados de firma digital y* `de` *para cifrado de datos.*
[40] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*



`<type of key>_isroot` [41] indica si el certificado generado será raíz (valor 1) o no (valor 0). La variable `subject` indica el campo titular del certificado X.509 que será generado. Si la variable `<type of key>_isroot` vale 1, la aplicación asignará el valor de la variable `subject` al campo emisor del certificado.

En el caso de que las claves de master i3D fueran las de la TSA, como se indica en el apéndice CPS de KeyOne 2.1, entonces no se utilizará este fichero, y las claves i3D serán generadas y mantenidas en el HSM.

- KeyOne VA

El fichero `keyoneva_keys.def`[42] indica las propiedades de las claves y los certificados. La variable `keyAlgorithm`[43] especifica el algoritmo de cada tipo de clave. Por defecto, este algoritmo es RSA (valor `rsaEncryption`). Es posible cambiar este valor para generar claves DSA (en este caso el valor de la variable debe ser `id_dsa`). Si se indica claves DSA, es posible incluir los parámetros asociados en `keyParameters`[44] (si no se indican parámetros, la aplicación los generará de forma aleatoria). La variable `isroot`[45] indica si el certificado generado será raíz (valor 1) o no (valor 0). La variable `subject` indica el campo titular del certificado X.509 que será generado. Si la variable `isroot` vale 1, la aplicación asignará el valor de la variable `subject` al campo emisor del certificado.

El fichero `db_master_properties.txt`[46] indica las propiedades de las claves y los certificados de una entidad *master* i3D, en el caso de que tenga un PSS distinto al del componente VA. La variable `<type of key>_keyAlgorithm`[47] especifica el algoritmo de la clave. Por defecto, este algoritmo es RSA (valor `rsaEncryption`). Es posible cambiar este valor para generar claves DSA (en este caso el valor de la variable debe ser `id_dsa`). Si se indica claves DSA, es posible incluir los parámetros asociados en `<type of key>_keyParameters` [48] (si no se indican parámetros, la aplicación los generará de forma aleatoria). La variable `<type of key>_isroot` [49] indica si el certificado generado será raíz (valor 1) o

[41] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local* `ssl_online` *para SSL.*
[42] *Este fichero está ubicado en la carpeta data de la ruta de instalación del producto.*
[43] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*
[44] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*
[45] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*
[46] *Este fichero está ubicado en la carpeta* `scripts` *de la ruta de instalación del producto.*
[47] *Donde* `<type of key>` *indica el tipo de clave:* `ds` *para certificados de firma digital y* `de` *para cifrado de datos.*
[48] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*
[49] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*

no (valor `0`). La variable `subject` indica el campo titular del certificado X.509 que será generado. Si la variable `<type of key>_isroot` vale 1, la aplicación asignará el valor de la variable `subject` al campo emisor del certificado.

En el caso de que las claves de master i3D fueran las de la VA, como se indica en el apéndice CPS de KeyOne 2.1, entonces no se utilizará este fichero, y las claves i3D serán generadas y mantenidas en el HSM.

En la fase de puesta en marcha se crean los certificados raíz necesarios para los componentes KeyOne CA, KeyOne LRA, KeyOne TSA y KeyOne VA. Para hacer esto, debe utilizarse una de las utilidades de línea de comandos que incluye la tecnología KeyOne. Esta utilidad se llama `createpss.ws`[50] y, además de los certificados raíz, genera PSSs, claves privadas y, opcionalmente, los CSRs, dependiendo del tipo de entidad.

El *script* `createpss.ws` accede al fichero de propiedades para conocer las características de las claves y los certificados que generar. La función que genera los certificados raíz y que cumplen los requisitos que necesita esta función está relacionada con el *script* `createpss.ws y se` describe en la sección `Interface for creating the Private Secure Store` del capítulo `Cryptographic Support` del documento [FUNCSPEC].

Distribución de claves criptográficas utilizando certificados

Los certificados contienen la clave publica del titular de los mismos y son firmados por un tercero de confianza (Autoridad de certificación). Por esta razón es una manera segura de distribuir claves públicas.

La Autoridad de certificación de KeyOne genera certificados X.509v3 a partir de los datos de entrada que le envía la Autoridad de registro, o que están contenidos en una CSR (petición de certificado firmada) y de los parámetros de configuración de la aplicación previamente establecidos.

El proceso de generación de un certificado X.509 consiste en los dos pasos siguientes:

- Generación del campo `signature` del certificado X.509. El HSM (módulo hardware de seguridad) genera la firma de la estructura X.509 `toBeSigned` generada por el componente KeyOne CA. El HSM firma estos datos con la clave de firma de certificados de la CA que está guardada de forma segura en este hardware criptográfico. Por lo tanto, esta función se basa en este componente del entorno y la entrada, salida e información de error de esta función no se describen en este documento.

- Generación de la estructura X.509 `toBeSigned`. Esta función se consigue con el núcleo de KeyOne CA

  Las entradas de la funcionalidad de generación de certificados X.509 se corresponden con los datos principales que KeyOne CA necesita para generar un certificado X.509. Estos datos son los siguientes:

  - La clave pública del certificado. Esta clave asimétrica es generada y enviada por el componente Autoridad de registro en una estructura firmada.

---

[50] *El script createpss.ws está ubicado en la carpeta scripts en la ruta de instalación.*



- Información que debe aparecer en los campos o en las extensiones del certificado y que se generan en el sitio de registro, como por ejemplo el tipo de certificado o la política de aplicación en relación al certificado.

- Information previously configured and established from the certification site. An example of this can be the characteristics related to a certificate profile (fields and extensions, their values, …). This kind of information is configured in the KeyOne CA by an administrator, and is securely stored in the Private Secure Store.

- Información previamente configurada y establecida en el sitio de certificación. Un ejemplo de esto son las características relativas al perfil de certificación (campos y extensiones, sus valores ...). Este tipo de información se configura en KeyOne CA por un administrador u se almacena de forma segura en el almacén privado seguro.

La salida de la función de generación de certificados X.509 es un certificado X.509. Este certificado se almacena en la base de datos de KeyOne CA y también es devuelto a la entidad solicitante dentro de un lote KeyOne (KeyOne CA en el caso de lotes internos o KeyOne LRA en el caso de una Autoridad de registro solicitante).

Distribución de claves criptográficas distribuidas utilizando el directorio LDAP

Los certificados generados por KeyOne CA contienen las claves públicas de sus titulares. Estos certificados se pueden publicar en un directorio LDAP por lo que, en consecuencia, el protocolo LDAP es un método de distribución de claves.

La publicación de los certificados que genera KeyOne CA en un directorio LDAP es una funcionalidad opcional que se puede activar mediante la modificación de ciertos ficheros de configuración. Estas modificaciones de los ficheros de configuración son **módulos de personalización de KeyOne** que son parte del **entorno del sistema**. El documento [CONFGUIDE] describe la personalización relativa a la publicación de certificados X509 en directorios LDAP.

FCS_CKM.3.1

El sistema KeyOne accede a las claves criptográficas según las siguientes políticas organizativas:

- Política organizativa referente a la utilización autorizada de las claves, de acuerdo al requisito [KM3.5] del documento [CEN01b].

- Política organizativa referente a la confianza en certificados, de acuerdo al requisito [KM3.6] del documento [CEN01b].

Uso autorizado de claves

La política organizativa que se describe en el requisito [KM3.5] del documento [CEN01b] requiere que todas los utilizaciones autorizadas de las claves, se realicen durante la vida operativa de las mismas (como determine la política).

La tecnología KeyOne se basa en la utilización del PSS (almacén privado seguro) como repositorio de certificados y de otros datos sensibles. Los objetos firmados (como los certificados) sólo son válidos dentro de su vida operativa. Cuando se



alcanza la fecha de expiración el objeto no puede utilizarse nunca más y debe borrarse del PSS.

Esta función utiliza los siguientes mecanismos para borrar objetos caducados:

- En todos los accesos a objeto, el PSS recorre varios objetos hasta que encuentra el objeto requerido. Cualquier objeto inválido que el PSS encuentre durante esta búsqueda es borrado.
- No todos los objetos del PSS son validados cuando se busca un determinado objeto. Pueden quedar objetos inválidos en el PSS, pero estos objetos serán borrados la primera vez que alguien intente acceder a ellos.
- Cuando se abre el PSS, se borran de él todos los objetos inválidos.
- Los certificados expirados cuya clave privada está almacenada en el PSS no se borran, sino que se pasan al registro histórico[51] del PSS.

La función de validación de la expiración de certificados recibe como entrada el PSS en el que los certificados están almacenados. Esta función está integrada en el mecanismo descrito anteriormente y borrará o pasará al registro histórico del PSS los certificados cuya vida operacional haya caducado.

El resultado de esta función es distinto dependiendo del estado del certificado:

- Ninguno (el certificado es válido).
- El certificado se pasa al registro histórico del PSS (certificado expirado del que se tiene la clave privada asociada).
- El certificado expirado se elimina (no se dispone de la clave privada asociada al certificado).

Confianza en certificados

La política organizativa descrita en el requisito [KM3.6] del documento [CEN01b] requiere que antes de que el sistema KeyOne utilice un certificado de claves asimétricas de control[52] o de infraestructura[53], se asegure de que los certificados relacionados con estas claves siguen siendo válidos.

Cada vez que la tecnología KeyOne utiliza una clave el sistema verifica su validez. Además de la validación de la firma, también se realizan los siguientes controles:

- Expiración del certificado. Esta función relativa a este requisito se especifica en la sección Uso autorizado de claves.

---

[51] El registro histórico del PSS almacena certificados caducados y sus correspondientes claves privadas. Cuando un certificado caduca y el PSS lo detecta, se comprueba la existencia en el PSS de su clave privada. Si la clave privada está presente, el certificado y su clave privada se mueven al registro de histórico. De otro modo, el certificado se elimina.

[52] Las claves usadas por el personal gestionando o usando los componentes KeyOne VA, KeyOne CA y KeyOne TSA, y que pueden proveer servicios de autenticación, firma o confidencialidad, a personal interactuando con el sistema.

[53] Claves usadas por KeyOne VA, KeyOne CA y KeyOne TSA para procesos tales como autenticación de subsistemas, firma de registros de auditoría, cifrados transmitidos, …



- Revocación de certificados. Este requisito es garantizado por la función que verifica que los certificados contenidos en el PSS no están referenciados en la CRL que está instalada en el PSS. Cuando se instala una CRL en el PSS, todos los certificados se validan respecto a esta lista de certificados revocados. Si un certificado ha sido revocado, entonces se borra del PSS o se pasa al registro histórico del PSS (dependiendo de si se dispone de la clave privada asociada)

Estas funciones garantizan que antes de que el sistema KeyOne se apoye en certificados de claves asimétricas se asegura de que los certificados asociados a estas claves son aún válidos.

La instalación de CRLs en aquellos componentes que no las reciben automáticamente y en tiempo real, siguen las recomendaciones que se especifican en el apéndice CPS de KeyOne 2.1.

FCS_COP.1.1_1

El soporte criptográfico requiere que las operaciones criptográficas se realicen de acuerdo a un algoritmo específico y con unas claves criptográficas de tamaños específicos. Los algoritmos y los tamaños de claves especificados pueden basarse en un estándar asignado.

El sistema KeyOne realiza las siguientes operaciones criptográficas de acuerdo a los algoritmos criptográficos y los tamaños de claves que se especifican a continuación.

Los algoritmos que soporta la tecnología KeyOne son los siguientes:

- Cifrado y descifrado simétrico
  - DES (56 bits), 3DES (168 bits)
  - AES (128, 192, 256 bits)
  - RC2 (40, 64, 128 bits)
  - RC4 (128 bits)
- Cifrado asimétrico
  - Algoritmo simétrico y asimétrico
- Verificación de firma digital
  - RSA (512, 1024, 2048 bits) con SHA1
  - RSA (512, 1024, 2048 bits) con MD2
  - RSA (512, 1024, 2048 bits) con MD5
  - DSA (512, 1024 bits) con SHA1
- Generación y verificación de firma criptográfica simétrica
  - 3DES con SHA1
  - algoritmo HMAC
- Calculo de *hash* seguro: SHA1, MD2 y MD5

Los estándares y las recomendaciones relativas a los algoritmos especificados son los siguientes:

- RSA, PKCS #1 – RSA Encryption Standard
- DES, 3DES, FIPS 46-3, Data Encryption Standard
- DSA, FIPS PUB 186-2
- AES, FIPS PUB 197
- RC2, RFC 2268 – A description of the RC2 Encryption Algorithm
- SHA1, FIPS PUB 180-1
- MD5, RFC 1321 – The MD5 Message Digest Algorithm
- MD2, RFC 1319 – The MD2 Message Digest Algorithm
- HMAC, RFC 2104 – HMAC: Keyed-Hashing for Message Authentication
- La ejecución de estos algoritmos criptográficos tiene lugar en los siguientes procesos:
- Operaciones criptográficas en el almacén privados seguro
- Operaciones criptográficas relacionadas con el protocolo SSL/TLS
- Operaciones criptográficas relativas al mecanismo i3D
- Operaciones criptográficas relacionadas con los lotes KeyOne
- Operaciones criptográficas relacionadas con los mensajes NDCCP
- Operaciones criptográficas relacionadas con la generación de certificados y CRLs
- Operaciones criptográficas relacionadas con la firma de los TST
- Operaciones criptográficas relacionadas con la firma de mensajes OCSP
- Operaciones criptográficas relacionadas con la validación de la firma que está contenida en los mensajes CSR
- Operaciones criptográficas relacionadas con la generación de la firma digital contenida en los mensajes CSR

Algunos de estos procesos implican el uso de diferentes esquemas criptográficos algunos de los cuales son ejecutados por la tecnología KeyOne y otros son responsabilidad de los **componentes del entorno** (módulos de hardware criptográfico). Toda la criptografía se lleva a cabo por el software KeyOne, exceptuando las siguientes operaciones:

- Generación de firmas digitales asimétricas
- Descifrado asimétrico



Estas funciones son ejecutadas por componentes del entorno y la comunicación entre el sistema KeyOne y los módulos criptográficos se lleva a cabo utilizando la especificación PKCS #11[54].

Adicionalmente, el sistema KeyOne soporta el estándar organizativo sobre la generación de huellas digitales de certificados auto-firmados. Este estándar establece que la producción de huellas digitales de certificados auto-firmados utilice los algoritmos de *hash* definidos [ALGO]. Se recomiendan medidas adicionales, como la comprobación de la huella digital del certificado (valor *hash* calculado sobre el certificado auto-firmado) frente a la información obtenida a través de una ruta segura para tener garantías sobre la corrección de este certificado.

The fingerprint of a self-signed certificate can be reported in the following two cases:

La huella digital de un certificado auto-firmado se puede reportar en los dos casos siguientes:

- Instalación de un certificado auto-firmado en el almacén privado seguro.

  Por defecto, en la tecnología KeyOne, cuando un certificado auto-firmado se instala en el PSS, se reportan las huellas digitales SHA1 y MD5. Se pude inhibir la huella digital MD5 modificando los ficheros de configuración. Estas modificaciones de los ficheros de configuración son los **módulos de personalización KeyOne** que son parte del **entorno del sistema**. El documento [CONFGUIDE] describe la personalización relativa a la inhibición de las huellas digitales MD5.

- Visualización de un certificado auto-firmado que ya está instalado en el almacén privado seguro.

  La tecnología KeyOne reporta las huellas digitales SHA1 y MD5 de los certificados auto-firmados que están instalados en el almacén privado seguro. En este caso, el apéndice CPS de KeyOne 2.1 incluye la restricción de utilizar la huella digital SHA1 y no la MD5

La funcionalidad relativa a la generación de huellas digitales está involucrada en los siguientes procesos:

- Proceso de generación del PSS. Cuando se genera un PSS, pueden generarse certificados auto-firmados y, consecuentemente, se reportan las huellas digitales correspondientes. En este caso, la funcionalidad asociada a la generación de la huella digital está en el *script* que genera el PSS. El *script* `createpss.ws` genera un PSS y los certificados auto-firmados, si es necesario. Este *script* se describe en la sección `Interface for creating the Private Secure Store` del capítulo `Cryptographic Support` del documento [FUNCSPEC].

- Visualización de certificados instalados en el PSS. Mediante la aplicación de administración de KeyOne, se pueden visualizar los certificados instalados en el PSS, y consecuentemente, se reportan sus huellas digitales. En este caso, la funcionalidad asociada a la generación de la huella digital está en la aplicación de administración de KeyOne. La entrada relacionada con esta funcionalidad es el acceso a la opción Ver el contenido del PSS del menú Gestión del PSS y la selección del certificado auto-firmado que visualizar.

[54] *La librería PKCS #11 utilizada es provista por el fabricante de HSM.*

Cuando se selecciona esta opción la aplicación calculará el *hash* SHA1 sobre el certificado y reportarán el resultado en base64.

Operaciones criptográficas en el almacén privados seguro

El almacén privado seguro (PSS) es un objeto seguro en el que se pueden almacenar datos sensibles que deban protegerse del acceso y las modificaciones ilícitas (claves privadas, certificados, datos de configuración, etc). La implementación del PSS se puede hacer en diferentes medios: disco, tarjeta *smartcard* o dispositivo criptográfico. salt

Para acceder al PSS se requiere una contraseña de acceso. De la contraseña se deriva una clave, utilizando un valor de "sal" y un contador de iteraciones, siguiendo las recomendaciones PKCS #5. El esquema de cifrado subyacente utiliza una clave simétrica 3DES de 192 bits.

Las operaciones criptográficas relativas a la gestión del PSS son las siguientes:

- **Cifrado y descifrado utilizando el algoritmo simétrico 3DES**

  Los datos sensibles del PSS se cifran con la clave 3DES, por lo que cada vez que la aplicación necesita los datos protegidos del PSS, se ejecuta una operación de descifrado 3DES. Estas operaciones aseguran el servicio de confidencialidad del PSS.

- **Esquema de integridad utilizando *hashing* SHA1 y cifrado simétrico 3DES y verificación del resultado de integridad**

  La integridad del contenido del PSS se consigue calculando una firma simétrica de los datos del PSS[55]. Se calcula el *hash* SHA1 de todo el PSS utilizando el algoritmo SHA1; a continuación dicho *hash* se cifra con la clave que se genera a partir de la contraseña (3DES), y se almacena en la parte de firma del PSS. Con este esquema de protección no es posible modificar el contenido del PSS sin que se note. De la misma manera cuando se abre el PSS la firma simétrica se valida utilizando los algoritmos SHA1 y 3DES.

- **Generación de un esquema de integridad y verificación del resultado de integridad**

  Un esquema de integridad se aplica a los objetos firmados contenidos en el PSS (certificados, CRLs, ...). El *hash* SHA1 se calcula sobre el campo `tobeSigned` de estos objetos. Cuando se valida el PSS se comprueba la validez de este *hash*.

- **Verificación de firma digital**

  El PSS puede contener objetos firmados. Estos objetos pueden ser certificados, CRLs, ... La firma de los objetos firmados debe validarse antes de insertarlos en el PSS. Si la firma de un objeto no se puede validar, el objeto no será insertado. Los algoritmos que se utilizan para verificar firmas asimétricas dependen de los algoritmos que se utilizaron en el proceso de generación de las firmas. La tecnología KeyOne soporta los siguientes algoritmos en relación a la gestión de firmas: SHA1, MD5, MD2, RSA y DSA.

---

[55] *El contenido del PSS, excepto certificados y CRLs.*



Operaciones criptográficas relacionadas con el protocolo SSL/TLS

Varias de las comunicaciones que se establecen entre distintos componentes KeyOne y servidores implican el establecimiento de una comunicación SSL/TLS. Cada establecimiento de un canal SSL/TLS implica las operaciones criptográficas descritas en las recomendaciones SSL/TLS:

- Cifrado y descifrado asimétrico (sobre digital) de la clave de sesión.
- Cifrado y descifrado simétrico de los datos de la comunicación.
- Verificación de la firma digital de los certificados y CRLs.
- Computación de un HMAC de todos los datos de la comunicación.

Los detalles de cuando la tecnología KeyOne utiliza una comunicación SSL/TLS y las interfaces relativas a estos protocolos se encuentran en la sección `Generation of a SSL/TLS communication between KeyOne components` del capítulo `Cryptographic Support` del documento [FUNCSPEC].

Operaciones criptográficas relativas al mecanismo i3D

La tecnología i3D se basa en la utilización de firmas digitales y otras técnicas criptográficas para garantizar la integridad y el no repudio de la base de datos.

En los procesos criptográficos relacionados con la tecnología i3D tiene lugar la generación de claves simétricas (3DES de 192 bits).

Las operaciones criptográficas relacionadas con el proceso i3D son las siguientes:

- **Cifrado asimétrico**

  Cada vez que un usuario comienza una sesión[56] i3D con una tabla lógica se añaden dos registros a la tabla de sesión: la entrada de inicio de sesión y la entrada de final de sesión. Estos registros contienen varias columnas de control entre los cuales se incluye el identificador de sesión (columna `sessionid`). Este identificador es diferente para todas las sesiones i3D que inician los diferentes usuarios sobre la tabla lógica. Cuando comienza una sesión i3D, se genera una clave simétrica aleatoria 3DES de 192 bits. Recibe el nombre de clave de sesión.

  Esta clave i3D se almacena en el registro de inicio de sesión y se cifra asimétricamente con destino a los *masters* de la base de datos, de forma que sólo los *masters* puedan conocerla. El cifrado asimétrico implica la generación de la clave criptográfica simétrica i3D relacionada con el sobre digital.

  Los algoritmos que este proceso implica son los siguientes:

  - Algoritmo asimétrico que depende del algoritmo de la clave pública contenida en el certificado *master*.
  - Algoritmo 3DES que se utiliza para el cifrado simétrico.

- **Firma digital asimétrica**

[56] *Las operaciones están agrupadas en sesiones (sesiones i3D), y por tanto para consultar o realizar cambios en la tabla el usuario debe primeramente abrir una sesión con la tabla.*

La firma asimétrica del registro de inicio de sesión incluye el valor de la columna `signature` del registro de inicio de la sesión previa.

La firma asimétrica del registro de fin de sesión incluye el valor de la columna `signature` del registro de fin de la sesión previa.

Los algoritmos que este proceso implica dependen del algoritmo de la clave pública contenida en el certificado de firma digital del sujeto que hace la acción en la base de datos.

- **Firma digital simétrica**

  La actualización de un registro lógico causa la inserción de un registro histórico que contiene los nuevos datos del registro lógico y que está relacionado con el registro histórico previo del mismo registro lógico. El nuevo registro incluye información sobre el identificador de la sesión activa. El registro completo se firma simétricamente utilizando la clave de sesión. Esta firma simétrica se calcula utilizando una firma HMAC.

- **Cálculo de *hash***

  Cuando se cierra una sesión i3D, se modifica el registro de fin de sesión que se insertó en la tabla de sesión cuando dicha sesión comenzó. Concretamente se añade al registro, el *hash* acumulado de todos los registros históricos generados durante la sesión. El algoritmo de *hash* que se utiliza es SHA1.

Otros procesos relacionados con la tecnología i3D que implican la computación de estos algoritmos es la siguiente:

- Recuperación de la integridad de la sesión

  La recuperación de la integridad debe hacerse solamente suponiendo que uno o mas registros de una sesión determinada hayan sino modificados externamente (por un accidente o fraude) y que se quiera establecer nuevos datos como datos válidos (posiblemente después de modificarlos si esto se considera conveniente). Esta funcionalidad especial está reservado a las entidades *master* y debe realizarse mediante las herramientas i3D de línea de comandos.

  La recuperación de la integridad de una sesión requiere antes que la firma simétrica de los registros históricos se verifique correctamente. Esto se puede hacer manualmente mediante la actualización de la columna `hmac` de los registros históricos cuya firma no sea válida (el valor apropiado es proporcionado por la herramienta i3D) o simplemente eliminando estos registros históricos

  Una vez que cada registro histórico se ha verificado correctamente, la herramienta i3D recalcula todos sus *hash* acumulados y actualiza el valores de la columna `hashchain` del registro de fin de sesión. La columna `entrytype` también se actualiza. Finalmente el registro de fin de sesión se firma asimétricamente de nuevo utilizando el certificado de firma digital del *master*.

- Prueba de integridad

  La integridad de una base de datos i3D se puede verificar a varios niveles, lo cual condice a diferentes pruebas de integridad. Estas pruebas se pueden realizar con las herramientas i3D que se distribuyen con los productos KeyOne.



Algunas pruebas requieren el conocimiento de la clave de sesión. Esta clave se almacena cifrada en el registro de inicio de sesión con destino a los *masters*. En estos casos sólo un *master* podrá realizar la prueba. Por otra parte, las pruebas que no requieren el conocimiento de la clave de sesión pueden ser realizados por cualquier entidad (un *master*, el usuario que realizó la sesión o incluso otros usuarios).

Las pruebas de integridad que es posible realizar en una base de datos i3D son:

- Prueba de integridad de una sesión cerrada

  Mediante esta prueba se verifica la integridad de todos los registros históricos generados en una sesión i3D determinada, y se comprueba también que no se han insertado ni suprimido registros de forma fraudulenta.

  Bajo este supuesto la integridad de la sesión puede verificarse sin saber la clave de sesión, por lo tanto cualquier entidad puede ejecutar la prueba. Se requiere el certificado de firma digital del usuario que realizó la sesión. Si la sesión la cerró un *master* también se requiere el certificado de firma digital de ese *master*.

  Para implementar esta prueba, la herramienta de verificación primero comprueba la integridad de los registros de inicio y final de sesión, verificando sus firmas asimétricas (campo `signature`).

  Después, se examina de forma secuencial todos los registros históricos. Para ello se utiliza el campo numérico `sidorder`, que identifica de forma secuencial todos los registros históricos generados en una misma sesión. Una vez examinados los registros históricos, se calculan sus *hash* acumulados. Después se comprueba que el resultado concuerde con el valor guardado en el campo `hashchain` del registro de final de sesión (si la sesión no tiene ningún registro histórico, se verifica que el campo esté vacío).

- Prueba de integridad de una sesión abierta

  En el caso de sesiones i3D no-cerradas también es posible realizar la prueba de integridad de sesión. Para hacerlo es necesario, sin embargo, saber la clave de sesión correspondiente. Por lo tanto, sólo un *master* puede realizar esta prueba. Además, se requiere el certificado de firma digital del usuario que inició la sesión.

  Es aconsejable ejecutar las pruebas de integridad cuando todos los usuarios de las bases de datos se encuentren desconectados. Esto asegura que cualquier sesión que esté abierta permanezca inactiva. Sin embargo, esta prueba puede también ejecutarse sobre una sesión activa.

  Para ejecutar esta prueba, primero la herramienta de verificación comprueba la integridad de los registros de inicio y final de sesión, verificando su firma asimétrica (campo `signature`).

  Después se examinan de forma secuencial todos los registros históricos de la sesión. Para ello se utiliza el campo numérico `sidorder`, que identifica de forma secuencial todos los registros históricos generados en una misma sesión. Este campo también se utiliza para comprobar que no se han insertado o suprimido registros históricos intermedios de forma fraudulenta.

Adicionalmente, para cada registro histórico se verifica que el valor del campo `hmac` concuerde con la firma simétrica basada en la clave de sesión del resto de los campos.

- Prueba de integridad de la tabla de registros históricos

  Mediante esta prueba, se verifica la integridad de todas las sesiones i3D realizadas sobre una tabla lógica determinada, comprobando también que no se han insertado o suprimido de forma fraudulenta sesiones intermedias. Es necesario conocer los certificados de firma digital de todos los usuarios que han realizado sesiones sobre la tabla. Además, si hay sesiones que fueron cerradas por *masters*, debe conocerse los certificados de firma digital de estos *masters*.

  La prueba se implementa examinando en orden ascendente las sesiones del identificador de sesión (campo `sessionid`). Para cada sesión, se aplica la prueba de integridad de sesión. Si hay sesiones abiertas, solamente un *master* podrá verificarlas (con la posible vulnerabilidad anteriormente mencionada).

  Simultáneamente a la verificación de firma asimétrica de cada registro de inicio de sesión, se comprueba que el enlace entre sesiones sea correcto. Ello se consigue gracias a que la firma incluye el campo `signature` del registro de inicio de sesión anterior.

- Prueba de integridad de la tabla de consultas

  Esta prueba es una extensión de la prueba de integridad de la tabla de registros históricos que permite verificar adicionalmente que el contenido de la tabla de consultas sea correcto.

  Primero, se realiza la prueba anterior para verificar la integridad y los enlaces de todas las sesiones de la tabla. Seguidamente, se comprueba que los datos almacenados de manera codificada en el último registro de históricos de cada registro lógico (campo `info`) concuerden con los valores de los diferentes campos del correspondiente registro de la tabla de consultas. Si el último registro histórico indica que se ha suprimido el registro lógico (campo `deleted`), se comprueba que no haya ningún registro en la tabla de consultas asociado al registro histórico.

Operaciones criptográficas relacionadas con los lotes KeyOne

El componente aplicación de registro envía peticiones de certificación o de revocación a la aplicación KeyOne CA. La aplicación KeyOne CA envía los certificados generados o los resultados de la revocación a la aplicación KeyOne RA. Este intercambio de datos se realiza utilizando un formato propio: La estructura lote de KeyOne.

Los lotes son firmados por sus emisores y son verificados por sus receptores.

Las operaciones criptográficas relacionadas con los procesos de los lotes KeyOne son los siguientes:

- Generación de firma digital

  La firma asimétrica del lote se calcula y se incluye en su campo `signature`.



Los algoritmos que se utilizan en este proceso dependen del algoritmo de la clave pública contenida en el certificado digital del sujeto que realiza la acción sobre el lote.

- Verificación de la firma digital asimétrica

  La firma asimétrica del lote se verifica antes de que se procesen los datos que el lote contiene.

  Los algoritmos utilizados en este proceso dependen del algoritmo que se utilizó para realizar la firma.

Operaciones criptográficas relacionadas con los mensajes NDCCP

Comunicaciones entre KeyOne CA y KeyOne VA. KeyOne CA (servidor KeyOne CertStatus) accede a la base de datos de KeyOne CA, en la que se almacena la información sobre los estados de revocación. De vez en cuando, KeyOne VA envía peticiones a KeyOne CA (servidor KeyOne CertStatus) para obtener la lista de certificados cuyo estado haya cambiado durante el último lapso de tiempo. NDCCP (protocolo *Near Domain Cert-status Coverage*) es un protocolo propio de KeyOne, que se utiliza en la comunicación entre un módulo Database Updater (en KeyOne VA) y un módulo servidor CertStatus (en KeyOne CA).

Esta comunicación tiene lugar para mantener actualizada la base de datos de estados de la aplicación KeyOne VA.

Las principales características de este protocolo son:

- Utiliza HTTPS (HTTP protegido con TLS/SSL) como mecanismo de transporte de los mensajes que se intercambian. Por lo tanto, los mensajes NDCCP son incrustados dentro del cuerpo de los mensajes de petición y de respuesta de mensajes HTTP.
- Los mensajes del protocolo se codifican de forma textual (ASCII).
- La sintaxis de los mensajes del protocolo consiste en dos mensajes: mensaje de petición (solicitando las revocaciones) y mensaje de respuesta (información sobre nuevas revocaciones). Ambos tipos de mensajes son firmados por su remitente y la firma es verificada en el destino.

Las operaciones criptográficas relacionadas con los procesos de los mensajes NDCCP son los siguientes:

- Generación de firma digital asimétrica

  La firma asimétrica del mensaje se calcula y se incluye en el campo `signature` del mensaje.

  Los algoritmos que se utilizan en este proceso dependen del algoritmo de la clave pública contenida en el certificado de firma digital del sujeto que realiza la acción sobre el mensaje.

- Verificación de la firma digital asimétrica

  La firma asimétrica del mensaje se verifica antes de procesar el contenido del mismo.

Los algoritmos que se utilizan en este proceso dependen del algoritmo utilizado en la firma.

Operaciones criptográficas relacionadas con la generación de certificados y CRLs

La generación de certificados y de CRLs implica la generación de una firma digital asimétrica. Este proceso criptográfico se ejecuta por los componentes del entorno (módulos de hardware criptográfico) y la comunicación entre el sistema KeyOne y los módulos criptográficos se lleva a cabo utilizando la especificación PKCS #11[57].

El componente del entorno que se utiliza para esta función es el módulo de hardware de seguridad que está en KeyOne CA. KeyOne CA firma los certificados y las CRLs generadas utilizando la clave privada almacenada en el HSM. Puesto que esta función está localizada en un componente del entorno, las entradas, salidas y errores de la función no son aplicables.

Operaciones criptográficas relacionadas con la firma de los TST

La TSA genera TST (sellos de tiempo) relacionados con mensajes de petición TSP. Estos TST son estructuras firmadas que genera el componente TSA.

La generación de TST implica la generación de una firma digital asimétrica. Este proceso criptográfico es ejecutado por los **componentes del entorno** y la comunicación entre el sistema KeyOne y los módulos criptográficos se lleva a cabo utilizando la especificación PKCS #11[58].

El componente del entorno que es responsable de esta función es el módulo de hardware de seguridad que se encuentra en KeyOne TSA. KeyOne TSA firma los TST que se generan utilizando la clave privada que se almacena en el HSM. Puesto que esta función está localizada en un componente del entorno, las entradas, salidas y errores de esta función no son aplicables.

Operaciones criptográficas relacionadas con la firma de mensajes OCSP

La VA (Autoridad de validación) puede tener que validar (las peticiones OCSP – *Online Certificate Status Protocol* - pueden estar firmadas) mensajes de petición OCSP. En este caso esta funcionalidad invoca la función de verificación de firmas digitales. Los algoritmos utilizados se corresponden con los utilizados en la firma digital de la petición.

La VA genera respuestas OCSP (*Online Certificate Status Protocol*) que se corresponden con peticiones OCSP. Estas respuestas OCSP son estructuras firmadas que genera el componente VA.

La generación de respuestas OCSP implica la generación de una firma digital asimétrica. Este proceso criptográfico es ejecutado por los **componentes del entorno** y la comunicación entre el sistema KeyOne y los módulos criptográficos se lleva a cabo utilizando la especificación PKCS #11[59].

---

[57] *La librería PKCS #11 usada proviene del fabricante del HSM.*
[58] *La librería PKCS #11 usada proviene del fabricante del HSM.*
[59] *La librería PKCS #11 usada proviene del fabricante del HSM.*



El componente del entorno que es responsable de esta función es el módulo de hardware de seguridad que se encuentra en KeyOne VA. KeyOne VA firma las respuestas OCSP que se generan utilizando la clave privada que se almacena en el HSM. Puesto que esta función está localizada en un componente del entorno, las entradas, salidas y errores de esta función no son aplicables.

Operaciones criptográficas relacionadas con la validación de la firma que está contenida en los mensajes CSR

El componente CA puede tener que validar los mensajes CSR (peticiones de certificado firmadas). En estos casos esta funcionalidad invoca a la función de verificación de firmas digitales. Los algoritmos utilizados se corresponden con los utilizados en la firma digital de la petición

Operaciones criptográficas relacionadas con la generación de la firma digital contenida en los mensajes CSR

Los mensajes CSR (peticiones de certificado firmadas) pueden ser generadas en los componentes entidades/servidores (KeyOne CA, KeyOne VA, KeyOne TSA) o en el entorno de un sujeto.

En el primer caso, estos componentes están conectados a un módulo de hardware de seguridad donde se generan y almacenan las claves. En estos casos, aunque la estructura CSR es generada por la tecnología KeyOne, la firma de la estructura es generada por este componente externo. Consecuentemente este proceso criptográfico es ejecutado por los **componentes del entorno** y la comunicación entre el sistema KeyOne y los módulos criptográficos se lleva a cabo utilizando la especificación PKCS #11[60].

El componente del entorno que es responsable de esta función es el módulo de hardware de seguridad que se encuentra en los componentes KeyOne CA, KeyOne VA y KeyOne TSA. Estos servidores firman los mensajes CSR que generan utilizando la clave privada que se almacena en el HSM. Puesto que esta función está localizada en un componente del entorno, las entradas, salidas y errores de esta función no son aplicables.

En el segundo caso, este componente se conecta a un dispositivo de creación de firma (SDC) donde se generan y se almacenan las claves. En este caso, aunque la estructura CSR es generada por la tecnología KeyOne, la firma de la estructura es generada por este componente externo. Consecuentemente este proceso criptográfico es ejecutado por los **componentes del entorno** y la comunicación entre el sistema KeyOne y los módulos criptográficos se lleva a cabo utilizando la especificación PKCS #11[61].

El componente del entorno que es responsable de esta función es el dispositivo de creación de firma que está localizado en el componente KeyOne LRA. En este caso KeyOne LRA firma los mensajes CSR utilizando la clave privada que se guarda en el SDC. Puesto que esta función está localizada en un componente del entorno, las entradas, salidas y errores de esta función no son aplicables.

---

[60] *La librería PKCS #11 usada proviene del fabricante del HSM.*
[61] *La librería PKCS #11 usada proviene del fabricante del HSM.*

FIA – Identificación y autenticación

FIA_UID.1.1

El sistema KeyOne permite cancelar el proceso de identificación antes de que el usuario sea identificado.

Cuando se inicia el servidor de administración (mediante la ejecución de los ficheros `start.bat/start_nodb.bat` en las aplicaciones KeyOne CA/KeyOne TSA, el fichero `start.s` de la aplicación KeyOne VA, o ejecutando el fichero `start.bat` de la aplicación KeyOne LRA), el servidor KeyOne solicita diferentes informaciones. En este punto, (antes de que el usuario haya sido identificado) el usuario puede cancelar el proceso de identificación, deteniendo el servidor KeyOne que haya sido lanzado para identificar y autenticar al usuario. Si el proceso no se cancela y el usuario es satisfactoriamente identificado y autenticado la aplicación KeyOne comenzará.

FIA_UID.2.1

El sistema KeyOne requiere que cada usuario se identifique antes de permitir que, a petición de ese usuario, se realicen acciones adicionales que también estén controladas por la TSF.

En el proceso de identificación y autenticación, las aplicaciones KeyOne utilizan el módulo `LogonManager`. Este componente es un módulo de Scryptor que ofrece una interfaz de programación común, en Scryptor, para realizar aquellas operaciones sobre PSS que sean dependientes del tipo de PSS al que se accede.

Algunas operaciones (como la apertura del PSS) requieren la ejecución de algunos procesos que son dependientes del tipo de PSS antes de poder invocar a la operación. Por ejemplo, para abrir un PSS sobre un dispositivo criptográfico los usuarios deben aportar su tarjeta y proporcionar el correspondiente PIN, mientras que para un PSS sobre disco solamente se debe proporcionar una contraseña.

El módulo de Scryptor `LogonManager` aísla a las aplicaciones KeyOne de estos detalles y les permite trabajar con cualquier tipo de PSS sin necesidad de recurrir a una programación realizada específicamente para cada tipo de PSS. Además el soporte de nuevos tipos de PSS es fácil y no requiere la recodificación de ninguna aplicación (ni tan siquiera la recodificación del propio módulo `LogonManager`).

Los tipos de PSS que soporta el módulo `LogonManager` son:

- PSS sobre disco
- PSS sobre disco y sobre dispositivo criptográfico accesible mediante PKCS #11

PSS sobre un HSM nCipher utilizando los modelos de seguridad de Safelayer Cada uno de estos tipos de PSS es gestionado por un módulo `logon` específico. El módulo `LogonManager` utiliza un URI para localizar la información necesaria para acceder a un PSS en particular. Esta información incluye una identificación del tipo de PSS y de otros parámetros que varían para cada tipo de PSS, como la ruta a la librería PKCS #11.

El apéndice CPS de KeyOne 2.1 incluye un requisito sobre la utilización de almacenes privados seguros sobre dispositivos criptográficos (HSM/SDC).



El proceso de identificación en las aplicaciones KeyOne se lleva a cabo antes de arrancar el servidor que ofrece la funcionalidad completa del producto. Esta identificación se lleva a cabo mediante el nombre (nombre distinguido) que corresponda al titular del certificado.

Cuando se inicia el servidor de administración (mediante la ejecución de los ficheros `start.bat/start_nodb.bat` en las aplicaciones KeyOne CA/KeyOne TSA, el fichero `start.s` de la aplicación KeyOne VA, o ejecutando el fichero `start.bat` de la aplicación KeyOne LRA), el servidor KeyOne solicita diferentes informaciones; estas informaciones dependen del tipo de la aplicación:

- En la aplicación KeyOne LRA, la identificación se realiza utilizando la siguiente información:
  - Nombre (nombre distinguido) que corresponde al titular del certificado de la aplicación KeyOne LRA.
  - Nombre del PSS que se ha generado durante la fase de puesta en marcha by que corresponde a la aplicación que se inicia.
- En las aplicaciones KeyOne CA, KeyOne VA y KeyOne TSA, la identificación se realiza con el nombre del PSS que se generó durante la puesta en marcha del producto y que corresponde a la aplicación que se inicia.

FIA_UAU.2.1

El sistema KeyOne requiere que cada usuario sea autenticado satisfactoriamente antes de permitir que, a petición de ese usuario, se realicen acciones adicionales que también estén controladas por la TSF.

En los procesos de identificación y de autenticación, las aplicaciones KeyOne el módulo `LogonManager`. Este componente es un módulo de Scryptor que ofrece una interfaz de programación común, en Scryptor, para realizar aquellas operaciones sobre PSS que sean dependientes del tipo de PSS al que se accede.

Algunas operaciones (como la apertura del PSS) requieren la ejecución de algunos procesos que son dependientes del tipo de PSS antes de poder invocar a la operación. Por ejemplo, para abrir un PSS sobre un dispositivo criptográfico los usuarios deben aportar su tarjeta y proporcionar el correspondiente PIN, mientras que para un PSS sobre disco solamente se debe proporcionar una contraseña.

El módulo de Scryptor `LogonManager` aísla a las aplicaciones KeyOne de estos detalles y les permite trabajar con cualquier tipo de PSS sin necesidad de recurrir a una programación realizada específicamente para cada tipo de PSS. Además el soporte de nuevos tipos de PSS es fácil y no requiere la recodificación de ninguna aplicación (ni tan siquiera la recodificación del propio módulo `LogonManager`).

Los tipos de PSS que soporta el módulo `LogonManager` son:

- PSS sobre disco
- PSS sobre disco y sobre dispositivo criptográfico accesible mediante PKCS #11

PSS sobre un HSM nCipher utilizando los modelos de seguridad de Safelayer Cada uno de estos tipos de PSS es gestionado por un módulo `logon` específico. El módulo `LogonManager` utiliza un URI para localizar la información necesaria para acceder a un PSS en particular. Esta información incluye una identificación del tipo de PSS y de



otros parámetros que varían para cada tipo de PSS, como la ruta a la librería PKCS #11.

El apéndice CPS de KeyOne 2.1 incluye un requisito sobre la utilización de almacenes privados seguros sobre dispositivos criptográficos (HSM/SDC).

El proceso de identificación en las aplicaciones KeyOne se lleva a cabo antes de arrancar el servidor que ofrece la funcionalidad completa del producto. Esta identificación se lleva a cabo mediante el certificado de autenticación del sujeto que inicia la aplicación.

Cuando se inicia el servidor de administración (mediante la ejecución de los ficheros `start.bat/start_nodb.bat` en las aplicaciones KeyOne CA/KeyOne TSA, el fichero `start.s` de la aplicación KeyOne VA, o ejecutando el fichero `start.bat` de la aplicación KeyOne LRA), el servidor KeyOne solicita diferentes informaciones; estas informaciones dependen del tipo de la aplicación:

- En la aplicación KeyOne LRA, la autenticación se realiza utilizando la siguiente información:
  - Certificado de autenticación del administrador que inicia la aplicación.
  - La posesión de la tarjeta *smartcard* con el certificado correcto y el PIN que protege as dispositivo.
- En las aplicaciones KeyOne CA, KeyOne VA y KeyOne TSA, la autenticación se lleva a cabo utilizando tarjetas *smartcards* que permiten el acceso al servidor y los PIN que protegen este dispositivo.

FIA_UAU.6.1

El sistema KeyOne re-autentica a un usuario después de que éste finalice la sesión.

Cuando una usuario finaliza una sesión con una aplicación o servidor, la sesión se cierra y el contexto de la aplicación queda como cuando el usuario aún no había comenzado la sesión. En consecuencia, cuando el usuario trata de iniciar una nueva sesión , tiene que re-autenticarse con los mismos parámetros que en la sesión anterior.

En las aplicaciones KeyOne se requiere la autenticación antes de arrancar el servidor KeyOne que ofrece la funcionalidad completa del producto. Esta autenticación se lleva a cabo presentando el certificado de autenticación del administrador que intenta acceder.

El proceso de autenticación en las aplicaciones KeyOne se lleva a cabo antes de arrancar el servidor KeyOne que ofrece la funcionalidad completa del producto. Esta autenticación se lleva a cabo mediante el certificado de autenticación del sujeto que inicia la aplicación.

Cuando se inicia el servidor de administración (mediante la ejecución de los ficheros `start.bat/start_nodb.bat` en las aplicaciones KeyOne CA/KeyOne TSA, el fichero `start.s` de la aplicación KeyOne VA, o ejecutando el fichero `start.bat` de la aplicación KeyOne LRA), el servidor KeyOne solicita las siguientes informaciones:

- Nombre del PSS que se ha generado durante la fase de puesta en marcha del producto y que corresponde a la aplicación que se inicia.



- Secreto que corresponde al PSS. El PIN o PINs que protegen al dispositivo, si tal dispositivo se está utilizando para almacenar las claves del PSS. El apéndice CPS de KeyOne 2.1 incluye un requisito sobre la utilización de almacenes privados seguros sobre dispositivos criptográficos (HSM/SDC).
- Certificado de autenticación del administrador que inicia la aplicación.

FPT – Protección de las TSF

FPT_ITI.1.1

El sistema KeyOne proporciona la capacidad de detectar modificaciones de todos los datos TSF durante su transmisión entre las TSF y un producto IT de confianza dentro de la siguiente métrica: la fuerza de la detección de la modificación se basa en la fuerza de los algoritmos utilizados en el mecanismo KeyOne i3D.

Esta función también se aplica a las copias de seguridad generadas por el sistema. Esta copia de seguridad abarca la información del sistema sobre los sujetos y a todos los datos necesarios para restaurar el sistema después de un fallo o de un desastre y que están almacenados en el PSS o en las bases de datos de KeyOne.

Las copias de seguridad se protegen frente a la modificación utilizando firmas digitales, *hashes* que incluyen claves o códigos de autenticación.

Las copias de seguridad y los procesos de recuperación siguen las recomendaciones que se especifican en el apéndice CPS de KeyOne 2.1. Los mecanismos de seguridad que se aplican a los datos son los mismos que se aplican al almacén privado seguro y a la base de datos. Como se describe en las secciones `Cryptographic operations over the private secure store` y `Services related to the i3D technology` del capítulo `Cryptographic Support` del documento [FUNCSPEC], estos datos se protegen frente a la modificación.

La integridad de una base de datos i3D se puede verificar con la herramienta de línea de comandos `i3dverify.ws` que se proporciona con los productos KeyOne. Esta herramienta realiza la verificación utilizando algunos certificados y claves, según el tipo de prueba que se haga. Este *script* debe ejecutarse utilizando un intérprete de línea de comandos del sistema operativo desde la carpeta `scripts` de la carpeta de instalación del producto.

Otra parte de esta función está relacionada con la protección frente a virus y software malicioso para asegurar la integridad de los sistemas y que la información que procesan se preserva.

Gran parte de la funcionalidad de las aplicaciones KeyOne está implementada en *scripts* programados en el lenguaje Scryptor. Para garantizar su integridad estos ficheros son firmados.

Cuando una aplicación KeyOne se instala desde el CD de distribución, los *scripts* han sido ya firmados por Safelayer. Sin embargo, la puesta en marcha de la mayoría de los productos KeyOne requieren la modificación de algún *script* con la finalidad de fijar los parámetros de configuración. Después de modificarlos, la firma original de los *scripts* deja de ser válida. Para mantener la firma de los *scripts* modificados, dichos *scripts* deben firmarse de nuevo.



La función para mantener la integridad del sistema mediante la firma de *scripts* corresponde con el *script* `sign.ws`.

Por lo tanto, este mecanismo asegura la integridad del sistema KeyOne.

FPT_ITI.1.2

El sistema KeyOne proporciona la capacidad de verificar la integridad de todos los datos TSF durante su transmisión entre las TSF y un producto IT de confianza y de generar un informe si se detectan modificaciones.

Esta función también se aplica a las copias de seguridad generadas por el sistema. Esta copia de seguridad abarca la información del sistema sobre los sujetos y a todos los datos necesarios para restaurar el sistema después de un fallo o de un desastre y que están almacenados en el PSS o en las bases de datos de KeyOne.

Las copias de seguridad se protegen frente a la modificación utilizando firmas digitales, *hashes* que incluyen claves o códigos de autenticación.

Las copias de seguridad y los procesos de recuperación siguen las recomendaciones que se especifican en el apéndice CPS de KeyOne 2.1. Los mecanismos de seguridad que se aplican a los datos son los mismos que se aplican al almacén privado seguro y a la base de datos. Como se describe en las secciones `Cryptographic operations over the private secure store` y `Services related to the i3D technology` del capítulo `Cryptographic Support` del documento [FUNCSPEC], estos datos se protegen frente a la modificación.

La integridad de una base de datos i3D se puede verificar con la herramienta de línea de comandos `i3dverify.ws` que se proporciona con los productos KeyOne. Esta herramienta realiza la verificación utilizando algunos certificados y claves, según el tipo de test que se haga. Este *script* debe ejecutarse utilizando un intérprete de línea de comandos del sistema operativo desde la carpeta `scripts` de la carpeta de instalación del producto. Este *script* genera un informe que indica el estado de la verificación de la integridad.

La integridad del contenido del PSS se consigue calculando una firma simétrica de los datos del PSS[62]. Se calcula el *hash* SHA1 de todo el PSS utilizando el algoritmo SHA1; a continuación dicho *hash* se cifra con la clave que se genera a partir de la contraseña (3DES), y se almacena en la parte de firma del PSS. Con este esquema de protección no es posible modificar el contenido del PSS sin que se note. De la misma manera cuando se abre el PSS la firma simétrica se valida utilizando los algoritmos SHA1 y 3DES.

When the integrity over the PSS is verified and the outcome of the validation is unsuccessful, then a report of the status is reported.

FPT_ITC.1.1

El sistema KeyOne protege a todos los datos que se transmiten entre las TSF y un producto IT de confianza de la revelación no autorizada.

---

[62] *El contenido del PSS, excepto los certificados y CRLs.*



Los parámetros de seguridad que sean críticos y otras informaciones que sean confidenciales se guardan siempre cifradas. El cifrado satisface los requisitos de cifrado que se especifican en [ALGO].

Los procesos de copia de seguridad y de recuperación siguen las recomendaciones del apéndice CPS de KeyOne 2.1. Los mecanismos de seguridad que se aplican a los datos son los mismos que se aplican al almacén privado seguro y a la base de datos. Como se describe en las secciones `Cryptographic operations over the private secure store` y `Services related to the i3D technology` del capítulo `Cryptographic Support` del documento [FUNCSPEC], estos datos se protegen frente a la revelación no autorizada.

FPT_ITA.1.1

Las peticiones y reportes relativos a la revocación y/o suspensión se procesan de forma puntual. El máximo retraso entre la recepción de una petición de revocación y/o suspensión y la actualización de la información sobre el estado del certificado afectado no puede exceder un día (24 horas).

Nota: Rauth + MP < 24 Hrs, por lo que el sistema KeyOne es capaz de procesar peticiones dentro de MP.

Donde: Rauth es el tiempo de autenticación de la revocación (procedimental o automática); MP es el tiempo de propagación del mensaje de revocación desde el servicio de gestión de la revocación al servicio de estado de revocación (requerimiento del sistema KeyOne).

Las peticiones de revocación o suspensión pueden proceder tanto del servicio de registro de KeyOne LRA (usualmente) o del servicio de certificación de KeyOne CA. En ambos casos, si la petición de revocación es aceptada, la revocación deviene efectiva automáticamente para el sistema de certificación, y por tanto la base de datos de la CA contendrá la información sobre el nuevo estado del certificado.

El tiempo de propagación desde el servicio de gestión de la revocación hasta el servicio de estado de revocación implica la actualización del componente KeyOne VA.

El servidor KeyOne CertStatus (el componente KeyOne CA) accede a la base de datos de KeyOne CA en la que se almacena la información sobre los estados de revocación de los certificados. Cada cierto tiempo (parámetro de configuración) KeyOne VA enviará peticiones al servidor KeyOne CertStatus para obtener la lista de certificados que han cambiado su estado durante el último lapso de tiempo.

Además, se puede configurar un parámetro de KeyOne VA para establecer la respuesta que debe proporcionar el servidor OCSP cuando la base de datos caduca. Los valores posibles son los siguientes: `ignore` (en este caso no se devolverá ningún error), `try_later` e `internal_error`. El requisito asociado a esta función requiere que se registre la ausencia de datos de TSF cuando éstos se requieren y, por esta razón, los valores que se permite poner en este parámetro son `try_later` o `internal_error`. Puesto que todos los mensajes OCSP son registrados en la base de datos de KeyOne VA, la ausencia de datos de las TSF cuando son requeridos se registra en la base de datos.

La función de petición de cambio del estado de certificados se consigue de acuerdo al procedimiento descrito en el apéndice CPS de KeyOne 2.1. Puesto que



este documento especifica una recomendación sobre el tiempo de sincronización entre el servidor KeyOne CertStatus y KeyOne VA, la conformidad con el procedimiento relacionado asegura el cumplimiento de esta función. En este caso, este parámetro de sincronización debe ser igual al parámetro que define la caducidad de la base de datos.

Para sincronizar la información de revocación entre el servidor KeyOne CertStatus y el servidor KeyOne VA, la aplicación KeyOne VA debe configurarse. La configuración consiste en la etapa de validación que configura el módulo `databasestage`. La opción `Database expiration` permite especificar este tiempo expresado en segundos (la base de datos se considerará caducada si no se actualiza antes de que transcurra este número de segundos). La opción `Expired database` permite establecer la respuesta que dará el servidor OCSP cuando la base de datos expire. En este caso, los valores que se pueden establecer son: `try_later` o `internal_error`.

FDP – Protección de datos de usuario

FDP_DAU.1.1

KeyOne proporciona la capacidad de generar evidencias que garanticen la validez de la asociación entre los datos de usuario que se incluyen en una petición de certificación y la clave pública del usuario que solicita la certificación

Esta función implementa un mecanismo para obtener la prueba de posesión (PoP) para garantizar que la entidad que solicita la certificación está realmente en posesión de la clave privada que corresponde a la clave pública que se solicita certificar

Esta función incluye un bloque de firma en cada petición de certificado que se crea con la clave privada del operador de registro (aprobador de KeyOne LRA). Este operador garantiza que la petición de certificado corresponde realmente al usuario que solicita la certificación de la clave pública que está contenida en dicha petición de certificado. El mecanismo que implementa la PoP consiste en la generación, por un operador de registro, de un lote **firmado** que contiene la petición de certificación para la nueva clave generada.

Puesto que el lote firmado contiene los datos del usuario que están dentro de la petición de certificación y la clave pública para la que el usuario solicita la certificación, éste puede considerarse como una prueba que garantiza la asociación entre los datos del usuario y la clave pública

La clave que se utiliza para firmar la PoP es la establecida como clave de firma digital en el componente KeyOne LRA[63]. La clave de firma y el certificado deben ser válidos y deben estar instalados en el almacén privado seguro de KeyOne LRA. Este certificado de firma debe estar instalado en el componente KeyOne CA como una autoridad de registro reconocida.

El bloque de firma generado se inserta en el campo `signature` del lote que se envía mediante HTTPS a KeyOne CA.

---

[63] *Las propiedades para esta clave están especificadas en el fichero `lra_properties.txt` ubicado en la carpeta scripts folder en el directorio de instalación de KeyOne LRA.*



This function is related to the functionality of the batch signature in the KeyOne LRA site. The signed batch generated by the KeyOne LRA component in this function is the following:

Esta función está relacionada con la funcionalidad de la firma de lotes en el sitio de KeyOne LRA. El lote firmado que genera el componente KeyOne LRA es el siguiente:

- Información genérica de lote KeyOne

  La información genérica identifica el lote, su tipo de contenido y su estado actual.

  - `batchid`: Identificador del lote. Este campo identifica un lote entre todos los que genera una Autoridad de registro.
  - `batchtype`: Tipo de lote. Este campo identifica el tipo de lote de petición. Todas las peticiones de un lote deben ser de un mismo tipo. Un lote puede ser:
    - `CR`: Lote de certificación. Contiene peticiones de certificado.
    - `RR`: Lotes de revocación. Contiene peticiones de revocación.
    - `UR`: Lotes de actualización. Este tipo de lote se utiliza para el intercambio de información entre la RA y la CA.
  - `status`: Estado del lote. Este campo corresponde, aproximadamente, con la etapa del ciclo de vida en la que se encuentra el lote.

- Datos relativos a KeyOne RA

  La Autoridad de registro genera el lote e incluye en él datos que serán procesados por la CA. Estos datos incluyen peticiones de certificación o revocación, así como otros datos informativos que intercambiar

  Después de añadir estos datos, la RA firma el lote para garantizar que la CA los recibe sin que sean modificados por un tercero.

  La información que la RA añade al lote es la siguiente:

  - Información general:
    - `timereq`: Fecha y hora en la que el lote ha sido generado por la RA.
    - `rasubject`: Nombre distinguido de la RA que generó el lote.
    - `policiesReq`: Lista de todas los perfiles de certificación cuya aplicación se solicita. En un lote de certificación (CR), esta lista contiene los nombres de todos los perfiles de certificación que aparecen en las peticiones de certificación. Si el lote no es CR, este campo queda vacío.
  - CSRs

    La parte más importante de los datos que añade al lote la RA es la lista de peticiones.

- `csrReportSeq`: Lista de peticiones. En un lote CR contendrá peticiones de certificación. En un lote RR contendrá peticiones de revocación. En lotes de otro tipo este campo puede estar vacío.

- Argumentos

  Los argumentos son datos adicionales que la RA envía a la CA. Estos datos adicionales pueden ser información que la RA necesita recuperar una vez que la CA procese el lote, o bien otras informaciones que la CA pueda necesitar. En lotes UR, los argumentos contienen los datos que se intercambian. Los campos son:

  - `scryptorGenericReq`: Datos a enviar a la CA.

- Firma

  Después de añadir todos los datos al lote, la RA lo firma para asegurarse de que la CA reciba el lote sin que sea modificado por un tercero. El único campo aquí es:

  - `rasignature`: Firma del lote generada por la RA.

La funcionalidad relacionada con la generación de lotes RA se corresponde con la función que genera certificados desde el componente KeyOne LRA.

Si las peticiones de certificación proceden de componentes KeyOne, entonces las CSR serán generadas por el servidor KeyOne, normalmente en el mismo proceso en el que se genera el PSS (*script* `createpss.ws`). Puesto que las claves se generan y se almacenan bien en un HSM (módulo de seguridad hardware) o en un SCD (dispositivo de creación de firma), como se indica en el apéndice CPS de KeyOne 2.1, la firma relacionada con la petición de certificación (POP) se generará con este módulo criptográfico. En este caso la POP consiste en la firma relacionada con la petición de certificación firmada.

FDP_DAU.2.2

El Responsable de KeyOne CA tiene la habilidad de verificar evidencia de la validación de la información indicada en la función `FDP_DAU.1.1`, y tiene la habilidad de verificar la identidad del usuario que generó esta evidencia.

Antes de la generación del certificado, el sistema KeyOne asegura Prueba de Posesión.

El servicio implementa un mecanismo para obtener prueba de posesión (POP) para asegurar que el sujeto que solicita la certificación es realmente el poseedor de la clave privada relacionada a la clave pública contenida en el certificado. Este mecanismo consiste en la generación de la petición de certificación que es una Petición Firmada de Certificación (CSR).

- Si la petición de certificación viene de una Autoridad de Registro (componente KeyOne LRA), entonces la CSR será generada por el servidor de KeyOne LRA. Puesto que las claves del sujeto están generadas y almacenadas en un módulo criptográfico de tarjeta inteligente, tal y como se indica en el apéndice CPS de KeyOne 2.1, la firma relacionada a la petición de certificación (POP) será generada por el SCD (Dispositivo de Creación de Firma). La firma relacionada a la POP la lleva a cabo el operador de registro, y consiste en la firma del lote (con



los datos de la petición de certificación) firmado por el operador de registro, y enviada a la Entidad de Certificación. Esta firma está incluida en el campo `rasignature` (lote con firma *detached* generada por la Autoridad de Registro) del lote.

- Si la petición de certificación proviene de componentes KeyOne, entonces la CSR será generada por el servidor KeyOne, normalmente en el mismo proceso que en el paso de generación del PSS (script `createpss.ws`). Puesto que las claves se generan y se almacenan, bien en un HSM (módulo de seguridad hardware), bien en un SCD (Dispositivo de Creación de Firma), tal y como se indica en el apéndice CPS de KeyOne 2.1, entonces la firma relacionada a la petición de certificación (POP) será generada por este módulo criptográfico. En este caso, la POP consiste en firma relacionada a la Petición de Certificación Firmada.

La función que cumple esta funcionalidad verifica:

La firma digital incluida en `rasignature` del lote enviado a la Autoridad de Certificación, o

La firma digital incluida en la petición de certificación firmada.

La primera verificación se realiza cuando la Autoridad de Certificación (KeyOne CA) recibe un lote de certificación de la Autoridad de Registro (KeyOne LRA). Antes de procesarlo, KeyOne CA verifica la firma adjunta al lote recibido.

Cuando la Autoridad de Certificación (KeyOne CA) importa una petición de certificación para generar un certificado, antes de procesarlo, KeyOne CA verifica la firma adjunta a la petición de certificación firmada.

Sobre la verificación de la identidad del usuario que generó la evidencia, el Responsable de la Autoridad de Certificación tiene la habilidad de verificar esta identidad.

- Si la petición de certificación viene de una Autoridad de Registro (componente KeyOne LRA), entonces se genera un lote firmado por el operador de Autoridad de Registro. En la sección de Información General del lote, `rasubject` contiene el nombre distintivo de la Autoridad de Registro que generó el lote. Puesto que este lote se almacena en la base de datos de la CA, el Responsable de la Autoridad de Certificación siempre puede verificar esta identidad.

- Si la petición de certificación proviene de componentes KeyOne, entonces la CSR será generada por el servidor KeyOne; esta CSR contiene el Nombre Distintivo de la entidad que solicita la certificación. Cuando KeyOne CA procesa la petición de certificación, se genera un lote interno que contiene esta CSR. Puesto que este lote se almacena en la base de datos de la CA, el Responsable de la Autoridad de Certificación siempre puede verificar esta identidad.

FXT_XKM – Gestión de claves

FXT_XKM.1.3 –Generación de la clave

El módulo criptográfico de seguridad sólo genera claves de firma QC/NQC bajo al menos de dos personas.

Tal y como se describe en el apéndice CPS de KeyOne 2.1, las claves mencionadas anteriormente se generan y almacenan en un HSM (módulo de seguridad hardware), con control de N mínimo de personas de un total de control de M personas (N > 1).

Puesto que estas claves asimétricas se generan en **componentes de entorno** (módulos criptográfico de hardware), esta función queda fuera del TOE (la comunicación entre el sistema KeyOne y los módulos criptográficos se realiza utilizando la especificación de PKCS #11[64]). De todos modos, a pesar de que esta función es responsabilidad del entorno, la tecnología KeyOne debe adaptarse a este comportamiento: en los procesos de puesta en marcha de KeyOne CA, KeyOne VA y KeyOne TSA deben cambiarse algunos datos en los archivos de configuración de KeyOne, para poder generar un esquema N de M en HSM.

Esta configuración consiste en el ajuste del proceso de generación del PSS y la ejecución de la aplicación KeyOne:

- El proceso de generación de PSS (esquela N de M, donde el control de N mínimo de personas de un total de control de M personas, N > 1).

  N tarjetas inteligentes son necesarias para poder acceder las claves protegidas por el conjunto de tarjetas inteligentes del operador (OCS – Conjunto de Tarjetas del Operador), la aplicación `with-nfast`[65] debe ser ejecutada y el PSS debe ser generado utilizando el parámetro `uri` en la herramienta en línea de comandos `createpss.ws`.

  - Windows: `c:\nfast\bin\with-nfast -t createpss.ws -from` *`<properties_file>`* `-uri "sfly:///pkcs11/interface.ws?p11Path=c:/nfast/toolkits/pkcs11/cknfast.dll"`

- La ejecución de la aplicación KeyOne (esquema N de M, donde el control de N mínimo de personas de un total de control de M personas, N > 1).

  En las aplicaciones KeyOne que se inician a través del archivo `start<…>.bat`, es necesario modificar el archivo `start<…>.bat` para poder ejecutar la aplicación a través del programa `with-nfast`[66].

  - Windows (ejemplo del archivo `start_nodb.bat` en la aplicación KeyOne CA): `start c:\nfast\bin\with-nfast -t keyoneca.exe -server_url" https://localhost:8081" -configfile "./config_ca.ws" -nodb`

  En otras aplicaciones, la aplicación KeyOne debe ejecutarse a través de la aplicación `with-nfast`[67].

  - Windows: `c:\nfast\bin\with-nfast -t` *`<KeyOne application command line>`*

---

[64] *La librería PKCS #11 utilizado proviene del proveedor de HSM.*
[65] *Esta aplicación está proporcionada por el proveedor de HSM (Ncipher).*
[66] *El programa está proporcionada por el proveedor de HSM (Ncipher).*
[67] *Esta aplicación está proporcionada por el proveedor de HSM (Ncipher).*



FXT_XKM.1.7 – Generación de clave

Toda generación de clave, si es aplicable, también reúnen los requerimientos criptográficos especificados en [ALGO].

Esta función es aplicable a las Claves de Firma de QC/NQC, Claves de Infraestructura[68] y Claves de Control[69] de los componentes KeyOne CA, KeyOne LRA, KeyOne VA y KeyOne TSA.

Puesto que estas claves asimétricas se generan en **componentes de entorno** (módulos criptográfico de hardware), esta función queda fuera del TOE (la comunicación entre el sistema KeyOne y los módulos criptográficos se realiza utilizando la especificación de PKCS #11). Los componentes de entorno implicado en el sistema son los siguientes:

- **Módulo de seguridad hardware** ubicado en KeyOne CA, KeyOne VA y KeyOne TSA. Este módulo crea y almacena loas claves relacionadas a la entidad relacionada con estos componentes.
- **Dispositivo de creación de firma** ubicado en el componente de Registro. Este dispositivo crea y almacena las claves del sujeto.

De todos modos, a pesar de que esta función es responsabilidad del entorno, la tecnología KeyOne debe ser adaptada a este comportamiento: durante el proceso de puesta en marcha de KeyOne CA, KeyOne LRA, KeyOne VA y KeyOne TSA puede que sea necesario cambiar algunos datos en los archivos de configuración de KeyOne para generar las claves con diferentes algoritmos a aquellos indicados en los archivos predeterminados.

El algoritmo aplicado para la generación de las claves identificadas anteriormente pueden ser configuradas e los archivos de propiedades de los componentes KeyOne. Para cada componente y servidor, un archivo de propiedades especifica las características para las claves y los certificados pata la entidad relacionada. Este archivo se usará como un parámetro de entrada para el *script* que generará las claves y los certificados.

- KeyOne CA

  El archivo `<type of entity>_ca_properties.txt`[70] indica las propiedades de las claves y de los certificados. La variable `<type of key>_keyAlgorithm`[71] especifica el algoritmo de clave. De forma predeterminada, este algoritmo

[68] *Claves utilizadas por KeyOne VA, KeyOne CA y KeyOne TSA para procesos como autenticación del subsistema, firma de registros de auditoría, cifrado transmitido, …*

[69] *Claves utilizadas por personal gestionando o utilizando los componentes KeyOne VA, KeyOne CA y KeyOne TSA, y que pueden proporcionar autenticación, firma o confidencialidad para personal que interactúa con el sistema.*

[70] `<type of entity>` *indica el tipo de entidad propietaria de las claves y de los certificados (*`root_ca` *corresponde a la Autoridad de Certificación raíz,* `root_online` *corresponde a una Autoridad de Certificación* online *raíz,* `subord_ca` *corresponde a una Autoridad de Certificación subordinada, y* `subord_online` *corresponde a una Autoridad de Certificación* online *subordinada). Este archivo está ubicado en la carpeta de* scripts *de la ruta de acceso a la instalación del producto.*

[71] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRL,* `ds` *para certificados de firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*

corresponde al algoritmo de RSA (valor `rsaEncryption`). Es posible cambiar este valor para generar claves de DSA (en este caso, el valor para esta variable debe ser `id_dsa`).

El archivo `db_master_properties.txt`[72] indica las propiedades de las claves para una entidad de máster de i3D, si tiene un PSS separado del componente de CA. La variable *<type of key>*`_keyAlgorithm`[73] especifica el algoritmo de clave. De forma predeterminada, este algoritmo corresponde al algoritmo de RSA (valor `rsaEncryption`). Es posible cambiar este valor para poder generar claves de DSA (en este caso, el valor para esta variable debe ser `id_dsa`).

En caso de que las claves de máster de i3D fueran las claves relacionadas a la entidad de CA, como se indica en el apéndice CPS de KeyOne 2.1, entonces este archivo no se utilizará, y las claves de i3D se generarán y mantendrán en el HSM.

- KeyOne LRA

  El archivo `lra_properties.txt`[74] indica las propiedades de las claves y de los certificados. La variable *<type of key>*`_keyAlgorithm`[75] especifica el algoritmo de clave. De forma predeterminada, este algoritmo corresponde al algoritmo de RSA (valor `rsaEncryption`).

- KeyOne TSA

  El archivo *<type of entity>*`_tsa_properties.txt`[76] indica las propiedades de las claves y de los certificados. La variable *<type of key>*`_keyAlgorithm`[77] especifica el algoritmo de clave. De forma predeterminada, este algoritmo corresponde al algoritmo de RSA (valor `rsaEncryption`). Es posible cambiar este valor para generar la clave DSA (en este caso, el valor para esta variable debe ser `id_dsa`).

  El archivo `db_master_properties.txt`[78] indica las propiedades de las claves y de los certificados para una entidad de máster de i3D, si tiene un PSS separado del componente de CA. La variable *<type of key>*`_keyAlgorithm`[79] especifica el algoritmo de clave. De forma predeterminada, este algoritmo corresponde al algoritmo de RSA (valor `rsaEncryption`). Es posible cambiar este

---

[72] *Este archivo está ubicado en la carpeta* scripts *de la ruta de acceso de instalación del producto.*
[73] *Donde* `<type of key>` *indica el tipo de clave:* `ds` *para certificados de firma digital y* `de` *para cifrado de datos.*
[74] *Este archivo está ubicado en la carpeta de* scripts *de la ruta de acceso de instalación del producto.*
[75] *Donde* `<type of key>` *indica el tipo de clave:* `ds` *para certificados de firma digital,* `de` *para cifrado de datos y* `ssl_local` *para SSL local.*
[76] *Este archivo está ubicado en la carpeta de* scripts *de la ruta de acceso de instalación del producto.*
[77] *Donde* `<type of key>` *indica el tipo de clave:* `ds` *para certificados de firma digital y* `de` *para cifrado de datos y* `ssl_local` *para SSL local.*
[78] *Este archivo está ubicado en la carpeta de* scripts *de la ruta de acceso de instalación del producto.*
[79] *Donde* `<type of key>` *indica el tipo de clave:* `ds` *para certificados de firma digital y* `de` *para cifrado de datos.*



valor para poder generar claves de DSA (en este caso, el valor para esta variable debe ser `id_dsa`).

En caso de que las claves de máster de i3D fueran las claves relacionadas a la entidad de CA, como se indica en el apéndice CPS de KeyOne 2.1, entonces este archivo no se utilizará, y las claves de i3D se generarán y mantendrán en el HSM.

- KeyOne VA

  El archivo `keyoneva_keys.def`[80] indica las propiedades de las claves y de los certificados. La variable `keyAlgorithm` especifica el algoritmo de clave para cada tipo de clave. De forma predeterminada, este algoritmo corresponde al algoritmo de RSA (valor `rsaEncryption`). Es posible cambiar este valor para poder generar claves de DSA (en este caso, el valor para esta variable debe ser `id_dsa`).

  El archivo `db_master_properties.txt`[81] indica las propiedades de las claves y de los certificados para una entidad de máster de i3D, si tiene un PSS separado del componente de CA. La variable *<type of key>*`_keyAlgorithm`[82] especifica el algoritmo de clave. De forma predeterminada, este algoritmo corresponde al algoritmo de RSA (valor `rsaEncryption`). Es posible cambiar este valor para poder generar claves de DSA (en este caso, el valor para esta variable debe ser `id_dsa`).

  En caso de que las claves de máster de i3D fueran las claves relacionadas a la entidad de CA, como se indica en el apéndice CPS de KeyOne 2.1, entonces este archivo no se utilizará, y las claves de i3D se generarán y mantendrán en el HSM.

En la fase de puesta en marcha, se crea el PSS relacionado a KeyOne CA, KeyOne LRA, KeyOne TSA y KeyOne VA. Para hacer esto, se debe usar una de las utilidades de en línea de comandos incluidas con la tecnología KeyOne. Esta utilidad se llama `createpss.ws`[83] y además del PSS, generará las claves privadas y opcionalmente los certificados dependientes del tipo de CA. Puesto que estas claves se generan y almacenan en HSM, la tecnología KeyOne debe invocar una función de generación de claves de HMS a través de la API PKCS #11. El *script* `createpss.ws` leyó el archivo de propiedades para conocer las características de las claves y certificados a generar. La función que genera un PSS (función que invoca la generación de claves simétricas) se describe en la sección `Interface for creating the Private Secure Store` del capítulo `Cryptographic Support` en el documento [FUNCSPEC].

---

[80] *Este archivo está ubicado en la carpeta data de la ruta de acceso de instalación del producto.*
[81] *Este archivo está ubicado en la carpeta* scripts *de la ruta de acceso de instalación del producto.*
[82] *Donde* `<type of key>` *indica el tipo de clave:* `ds` *para certificados de firma digital y* `de` *para cifrado de datos.*
[83] *El* script `createpss.ws` *está ubicado en la carpeta* scripts *de la ruta de acceso de instalación del producto.*



FXT_XKM.3.1 – Uso de clave

Controles de acceso están en lugar para todos los módulos criptográficos de seguridad utilizados para las siguientes claves:

- Claves de firma de QC.
- Claves de infraestructura (claves utilizadas por KeyOne VA, KeyOne CA y KeyOne TSA para procesos como autenticación del subsistema, firma de registros de auditoría, cifrado transmitido, …).
- Claves de control (claves utilizados por personal gestionando o utilizando los componentes KeyOne VA, KeyOne CA y KeyOne TSA, y eso puede proporcionar autenticación, servicios de firma o confidencialidad para personal interactuando con el sistema).

Tal y como se describe en el apéndice CPS de KeyOne 2.1, las claves referidas anteriormente se generan y almacenan en un HSM (Módulo de seguridad hardware), con control de N mínimo de personas de un total de control de M personas.

Puesto que estas claves asimétricas se generan en **componentes de entorno** (módulos criptográfico de hardware), esta función queda fuera del TOE (la comunicación entre el sistema KeyOne y los módulos criptográficos se realiza utilizando la especificación de PKCS #11[84]).

De todos modos, a pesar de que esta función es responsabilidad del entorno, la tecnología KeyOne debe adaptarse a este comportamiento. Esta configuración consiste en un ajuste del proceso de generación del PSS y del tipo de ejecución de la aplicación KeyOne:

- Proceso de generación del PSS (esquema N de M, donde el control de N mínimo de personas de un total de control de M personas, N > 1).

  Si son necesarias N tarjetas inteligente para poder acceder a las claves protegidas por el conjunto de tarjetas inteligentes de operador (OCS – Conjunto de Tarjetas de Operador), la aplicación `with-nfast`[85] debe ser ejecutada y el PSS debe ser generado utilizando el parámetro `uri` en la herramienta en línea de comandos `createpss.ws`.

  - Windows: `c:\nfast\bin\with-nfast -t createpss.ws -from <properties_file> -uri "sfly:///pkcs11/interface.ws?p11Path=c:/nfast/toolkits/pkcs11/cknfast.dll"`

- La ejecución de la aplicación KeyOne (esquema N de M, donde el control de N mínimo de personas de un total de control de M personas, N > 1).

  En las aplicaciones KeyOne que se inician por el archivo `start<…>.bat`, es necesario modificar el archivo `start<…>.bat` para poder ejecutar la aplicación a través del programa `with-nfast`[86].

---

[84] *La librería PKCS #11 utilizada es del proveedor de HSM.*
[85] *Esta aplicación está proporcionada por el proveedor de HSM (Ncipher).*
[86] *Programa proporcionada por el proveedor de HSM (Ncipher).*



- Windows (ejemplo del archivo `start_nodb.bat` en la aplicación KeyOne CA): `start c:\nfast\bin\with-nfast –t keyoneca.exe –server_url" https://localhost:8081" -configfile "./config_ca.ws" –nodb`

En otras aplicaciones, la aplicación KeyOne debe ser ejecutada a través de la aplicación `with-nfast`[87].

- Windows: `c:\nfast\bin\with-nfast –t <KeyOne application command line>`

FXT_XKM.6.5 – Almacén de claves, copias de seguridad y recuperación

El sistema KeyOne asegura que las copias de seguridad, almacén y recuperación de las siguientes claves sólo se lleva a cabo por personal autorizado:

- Claves de firma de QC.
- Claves de infraestructura (claves utilizadas por KeyOne VA, KeyOne CA, KeyOne TSA y KeyOne LRA para procesos como autenticación del subsistema, firma de registros de auditoría, cifrado transmitido, …).
- Claves de control (claves utilizados por personal gestionando o utilizando los componentes KeyOne VA, KeyOne CA, KeyOne TSA y KeyOne LRA y eso puede proporcionar autenticación, servicios de firma o confidencialidad para personal interactuando con el sistema).

La funcionalidad del Almacén de Claves relacionada a esta función es aplicable a la QC/ Claves de Firma de QC/NQC, Claves de Infraestructura [88] y Claves de Control [89] de los componentes KeyOne CA, KeyOne LRA, KeyOne VA y KeyOne TSA.

Esta función es aplicable a estas claves criptográficas asimétricas. Puesto que no existe ningún objetivo de seguridad que requiera esta función concerniente a las claves criptográficas simétricas, esta funcionalidad no es aplicable a claves simétricas.

Esta función cumple a través de la aplicación de **control de acceso** en el almacén, copias de seguridad y recuperación de las claves anteriores.

Control de acceso en el almacén de claves

- Claves de firma QC/NQC, y claves de Infraestructura de KeyOne CA, KeyOne VA y KeyOne TSA

  Puesto que las claves descritas anteriormente sólo se generan y almacenan en un módulo criptográfico de hardware, como se indica en el apéndice CPS de KeyOne 2.1, la función de almacén está basada en este **componente de entorno,** y por lo tanto esta función queda fuera del TOE (la comunicación entre

---

[87] Esta aplicación está proporcionada por el proveedor de HSM (Ncipher).
[88] Claves utilizadas por KeyOne VA, KeyOne CA y KeyOne TSA para procesos como una autenticación del subsistema, firma de registros de auditorías, transmisión de cifrados, …
[89] Claves utilizadas por personal gestionando o utilizando los componentes KeyOne VA, KeyOne CA y KeyOne TSA, y que pueden proporcionar autenticación, firma o confidencialidad para personal interactuando con el sistema.

el sistema KeyOne y los módulos criptográficos se realiza utilizando la especificación de PKCS #11[90]). El módulo de seguridad hardware ubicando en los componentes KeyOne CA, KeyOne VA y KeyOne TSA crea y almacena las claves relacionadas a las entidades asociadas a estos componentes. En este caso, como especifica el apéndice CPS de KeyOne 2.1, el HSM para el sistema KeyOne cumplirá con el estándar FIPS 140-2 nivel 3.

De todos modos, a pesar de que esta función es responsabilidad del entorno, la tecnología KeyOne debe adaptarse a este comportamiento. Esta configuración consiste en el ajuste del proceso de generación del PSS y la ejecución de la aplicación KeyOne:

- Proceso de generación del PSS (esquema N de M, donde el control de N mínimo de personas de un total de control de M personas, N > 1).

  Si N tarjetas inteligentes son necesarias para poder acceder las claves protegidas por el conjunto de tarjetas inteligentes de operador (OCS – Conjunto de Tarjetas de Operador), la aplicación `with-nfast`[91] debe ser ejecutada y el PSS debe ser generado utilizando el parámetro `uri` en la herramienta en línea de comandos `createpss.ws`.

  - Windows: `c:\nfast\bin\with-nfast -t createpss.ws -from` *`<properties_file>`* `-uri “sfly:///pkcs11/interface.ws?p11Path=c:/nfast/toolkits/pkcs11/cknfast.dll”`

- La ejecución de la aplicación KeyOne (esquema N de M, donde el control de N mínimo de personas de un total de control de M personas, N > 1).

  En aplicaciones KeyOne que se inician a través del archivo `start<…>.bat`, es necesario modificar el archivo `start<…>.bat` para poder ejecutar la aplicación a través del programa `with-nfast`[92].

  - Windows (ejemplo del archivo `start_nodb.bat` en la aplicación KeyOne CA): `start c:\nfast\bin\with-nfast -t keyoneca.exe -server_url” https://localhost:8081” -configfile “./config_ca.ws” -nodb`

  En otras aplicaciones, la aplicación KeyOne debe ser ejecutada a través de la aplicación `with-nfast`[93].

  - Windows: `c:\nfast\bin\with-nfast -t` *`<KeyOne application command line>`*

- Las claves de control de los componentes KeyOne CA, KeyOne VA y KeyOne TSA, y claves de Control e Infraestructura en el componente KeyOne LRA.

  Estas claves se generan y almacenan en un módulo criptográfico de hardware, a como se indica en el apéndice CPS de KeyOne 2.1, entonces la función de almacén se basa en este **componente de entorno**, y por lo tanto, esta función

---

[90] *La librería PKCS #11 utilizadas es del proveedor de HSM.*
[91] *Esta aplicación está proporcionada por el proveedor de HSM (Ncipher).*
[92] *Programa proporcionado por el proveedor de HSM (Ncipher).*
[93] *Esta aplicación está proporcionada por el proveedor de HSM (Ncipher).*



queda fuera de este TOE (la comunicación entre el sistema KeyOne y los módulos criptográficos se realiza utilizando la especificación de PKCS #11). El módulo criptográfico crea y almacena estas claves relacionadas a las entidades asociadas con estos componentes. En este caso, el control de acceso se basa en la posesión de los módulos criptográficos (tarjetas inteligentes) que contienen estas claves, y conocimiento del secreto para poder acceder al módulo criptográfico (PIN).

Control de acceso en procesos de copias de seguridad y recuperación

- Claves de firma de QC/NQC, y claves de Infraestructura de KeyOne CA, KeyOne VA y KeyOne TSA

  Puesto que las claves descritas anteriormente sólo se generan y se almacenan en un módulo criptográfico de hardware, como se indica en el apéndice CPS de KeyOne 2.1, entonces las funciones de copia de seguridad y de recuperación se basan en este **componente de entorno**, y por lo tanto esta función queda fuera de este TOE (la comunicación entre el sistema KeyOne y los módulos criptográficos se realiza utilizando la especificación de PKCS #11[94]). En este caso, como especifica el apéndice CPS de KeyOne 2.1, el HSM para el sistema KeyOne cumplirá el estándar FIPS 140-2 nivel 3.

- Claves de control de los componentes KeyOne CA, KeyOne VA y KeyOne TSA, y claves de Control y de Infraestructura en el componente KeyOne LRA.

  Puesto que estas claves se generan y almacenan en un módulo criptográfico de tarjeta inteligente, y cumpliendo con el estándar ITSEC E4, como se indica en el apéndice CPS de KeyOne 2.1, entonces el proceso de copia de seguridad y de recuperación no son aplicables en este tipo de claves.

FXT_XKM.6.7 – Almacén de clave, copia de seguridad y recuperación

El sistema KeyOne no contiene funciones que permiten hacer una copia de seguridad de las claves firma del titular o dejarlas en depósito (claves privadas).

Este requerimiento se asegura en la arquitectura de KeyOne por los componentes KeyOne LRA y KeyOne CA. Las claves de firma del titular se generan en el dispositivo de creación de firma (SCD) ubicada en el Componente de Registro. En este caso, como se especifica en el apéndice CPS de KeyOne 2.1, el SCD para el sistema KeyOne cumplirán con el estándar ITSEC E4. El depósito o la copia de seguridad por un componente externo al dispositivo del usuario es queda inhibido en estos dispositivos.

FXT_XKM.7.1 – Archivo de claves

El sistema KeyOne no contiene funciones que permiten el archivo de las claves de firma del titular (claves privadas).

Este requerimiento queda asegurado por la arquitectura de KeyOne compuesta por los componentes KeyOne LRA y KeyOne CA. Las claves de firma del titular se

[94] *Programa proporcionado por el proveedor de HSM (Ncipher).*

generan en el dispositivo de creación de firma (SCD) ubicado en el Componente de Registro. En este caso, como especifica el apéndice CPS de KeyOne 2.1, el SCD para el sistema KeyOne cumplirá con el estándar ITSEC E4. El archivo de claves queda inhibido en estos dispositivos.

FXT_XCG – Servicio de Generación de Certificados

FXT_XCG.1.1 - Generación de Certificados

El Servicio de Generación de Certificados asegura la integridad, autenticidad del origen de los datos, y cuando sea necesario, la privacidad y confidencialidad del mensaje de petición de certificado.

Todas las comunicaciones entre los componentes KeyOne LRA y KeyOne CA se realizan utilizando los Lotes de KeyOne. El originador del lote siempre firma estos lotes, y previo al procesado del lote, el destinatario debe verificar la firma digital del lote. El lote de KeyOne contiene el mensaje de petición de certificado, y consecuentemente proporciona todos los servicios de seguridad que proporcionan.

La firma del lote garantiza la **integridad** y la **autenticidad del origen de los datos** del mensaje de petición de certificado.

Entre el servidor KeyOne LRA y el servidor de KeyOne CA online, se establece una conexión SSL/TLS con autenticación de cliente (KeyOne CA online actuando como un servidor SSL/TSL).

Para establecer esta conexión SSL/TSL con autenticación de cliente, los siguientes dos tipos de certificados, correspondientes a las claves de Infraestructura, son necesarios:

- El certificado de servidor de SSL de CA online. Este certificado está presente en el PSS de KeyOne CA para usarse en la comunicación SSL con el componente KeyOne LRA.
- El certificado de autenticación de LRA. Este certificado está presente en el PSS de KeyOne LRA para ser utilizado como certificado de cliente en la comunicación SSL con el componente KeyOne CA online.

El proceso de autenticación de la LRA también implica la verificación que el certificado de LRA pertenece a una Autoridad de Registro reconocida. El administrador de CA mantiene una lista con las autoridades de registro que puede comunicar con esta CA.

El uso de SSL/TLS en la comunicación entre KeyOne LRA y KeyOne CA, garantiza la **integridad**, **autenticidad de origen de los datos**, **privacidad** y **confidencialidad** del mensaje de petición de certificado.

Por lo tanto, los servicios de seguridad requeridos por esta función se cumple a través del uso del lote de firma por el operador de la Autoridad de Registro y a través del establecimiento del protocolo SSL/TLS con el servidor KeyOne CA online.

FXT_XCG.1.2 - Generación de Certificación

El mensaje se procesa de forma segura y se comprueba para confirmación con la Política de Certificado aplicable.



En términos de tecnología de KeyOne, una plantilla de certificación, también llamada política de certificación o simplemente política, es un conjunto de normas programables que definen restricciones sobre los tipos de peticiones de certificado que la CA acepta. Estas normas también definen las características de los certificados emitidos de ese tipo de petición (por ejemplo, extensiones de certificado).

Se aplica una plantilla de certificación a la petición de certificado antes de que el certificado sea emitido. La plantilla de certificación que se aplica a la petición la proporciona la Autoridad de Registro que emite los lotes de certificación que procesará KeyOne CA. KeyOne LRA debe indicar qué plantilla de certificación debe ser aplicada para cada lote de petición (esta información se almacena en el lote, junto con los datos de la petición). Además, es posible restringir la plantilla de certificación (políticas) que cada RA reconocida está autorizada a solicitar en los lotes que genera. Se debe definir un conjunto de políticas permitidas para cada RA para este propósito.

El cumplimiento de esta función incluye dos funcionalidades:

- Función de gestión para poder restringir la aplicabilidad de la platilla de certificación para Autoridades de Registro

  - Sólo platillas de certificación insertadas en la aplicación KeyOne CA pueden ser permitidas para Autoridades de Registro que enviaron los lotes de certificación a la CA. Políticas autorizadas para cada RA reconocida deben ser configuradas una vez que las plantillas de certificación han sido definidas, desde el menú de gestión de la RA.

    La aplicación de administración KeyOne CA proporciona la función para poder añadir una nueva plantilla de certificación. La nueva plantilla debe basarse en cualquiera de las plantillas de certificación genéricas definidas en el archivo de configuración `config_ca_certtemplates.ws` o cualquiera de las plantillas que están definidas actualmente. Los campos de la plantilla base se mostrarán como campos predeterminados para la nueva plantilla. De todos modos, no se mantiene ninguna relación entre las dos plantillas una vez que se ha creado la nueva plantilla. Esta funcionalidad está disponible desde la opción `Add` del menú `Policies` de la aplicación de administración KeyOne CA. La información sobre las plantillas se almacena en el PSS.

  - Es posible definir el conjunto de plantillas de certificación que una RA reconocida concreta está autorizada a solicitar en lotes de certificación que genere. Si una RA solicita una plantilla de certificación para lo que no está autorizada, no será posible procesar el lote (KeyOne CA no mostrará ningún mensaje de error al cargar el lote en la base de datos de la CA, al intentar procesarlo). Al habilitar un certificado como una RA reconocida por primera vez, el conjunto de plantillas de certificación permitidas para esa RA quedará vacío. En la práctica, esto significa que ningún lote que venga de la RA puede ser procesado todavía, a pesar de que es una RA reconocida. Para que se puedan procesar lotes de RA, al menos una plantilla de certificación debe estar permitida para la RA. Si una de las plantillas de certificación que están permitidas para una o más RAs se elimina del conjunto de las plantillas de certificación de la CA (desde la pantallas de Políticas), será automáticamente eliminado del conjunto de de políticas permitidas de esas RAs. Esta funcionalidad está disponible desde la opción



`View list of recognized RAs` del menú `RA Management` de la aplicación de administración KeyOne CA. Información sobre la relación entre las platillas y las autoridades de registro reconocidas se almacenan en el PSS.

- La función que verifica la seguridad del mensaje, y comprueba la conformidad de la plantilla de certificación aplicable.

  Esta función verifica la firma digital relacionada con el lote, y comprueba si la plantilla solicitada está permitida para la Autoridad de Registro que la solicita. La entrada de esta función es información contenida en el lote de entrada, y el PSS. La función verifica la firma digital haciendo uso de los certificados contenidos en el PSS; esta función también usa la información contenida en el PSS relacionada con la aplicabilidad de la plantilla a la Autoridad de Registro.

FXT_XCG.1.3 - Generación de Certificación

Antes de la generación del certificado, el sistema KeyOne asegura Prueba de Posesión se valida.

El servicio implementa un mecanismo para obtener prueba de posesión (POP) para asegurar que el titular que solicita la certificación es el verdadero poseedor de la clave privada relacionada con la clave pública contenida en el certificado. Este mecanismo consiste en la generación de peticiones de certificación que es una Petición Firmada de Certificación (CSR).

- Si la petición de certificación viene de una Autoridad de Registro (componente KeyOne LRA), Entonces la CSR será generada por el servidor de KeyOne LRA. Puesto que las claves del titular se generan y se guardan en un módulo criptográfico de tarjeta inteligente, como se indica en el apéndice CPS de KeyOne 2.1, entonces la firma relacionada a la petición de certificación (POP) será generada por el SCD (Dispositivo de Creación de Firma). La firma relacionada al POP la lleva a cabo el operador de registro.

- Si la petición de certificación viene de componentes KeyOne, entonces la CSR será generada por el servidor KeyOne, normalmente en el mismo proceso que el paso de generación del PSS (*script* `createpss.ws`). Puesto que las claves se generan y se almacenan bien en un HSM (Módulo de Seguridad Hardware) o en un SCD (Dispositivo de Creación de Firma), como se indica en el apéndice CPS de KeyOne 2.1, entonces la firma relacionada a la petición de certificación (POP) será generada por este módulo criptográfico.

La función que cumple esta funcionalidad verifica la firma digital adjunta a la Petición Firmada de Certificación.

FXT_XCG.1.4 - Generación de Certificación

La clave utilizada para firmar un QC sólo debe ser utilizada para firmar QCs y, opcionalmente, los Datos de Estado de Revocación relacionados.

Las propiedades del certificado relacionado a la firma de QCs pueden ser especificadas en el proceso de generación del PSS de la CA. Para generar el PSS de la CA, debe utilizarse una de las utilidades en línea de comandos incluidas con



KeyOne CA. Esta utilidad se llama `createpss.ws`[95] y además del PSS, generará la clave privada de la CA y opcionalmente los certificados de la CA dependiendo del tipo de CA. El *script* `createpss.ws` trabaja a partir de un archivo de propiedades donde se especifica las propiedades de PSS a generar, al igual que las propiedades de los varios certificados propios que debe contener. Junto a `createpss.ws`, el archivo de propiedades de ejemplo se incluye para diversos tipos de entidades.

El archivo de propiedades que debe ser utilizado para crear el PSS de la CA es `root_ca_properties.txt`[96] (el archivo de propiedades para una CA online es el archivo `root_online_ca_properties.txt`) para CAs raíz y `subord_ca_properties.txt`[97] (el archivo de propiedades para una CA online es el archivo `subord_online_ca_properties.txt`) para CAs subordinadas. Las propiedades predeterminadas de la clave de firma de certificados especifica el valor para la extensión del uso de clave de `keyCertSign` y `cRLSign`. Este valor garantiza la generación de una clave de firma de QC para uso de firma de QCs y Datos de Estado de Revocación (CRLs). La variable de estos archivos de propiedades que contienen esta información es `csrs_extensions.keyUsage`.

La tecnología KeyOne garantiza el uso correcto de la extensión `keyUsage` de certificados que lo gestionan, y por lo tanto el uso de clave para firmar un QC sólo se utiliza para firmar QC y los Datos de Estado de Revocación relacionados.

FXT_XCG.1.6 - Generación de Certificación

Todos los certificados emitidos por el sistema KeyOne reúnen los requerimientos especificados en el Anexo 1 de [Eur99b]. En particular, están presentes las siguientes propiedades:

- Indicación del nombre o pseudónimo del titular.
- La clave pública en el certificado está relacionado a la clave privada del titular.
- La firma electrónica avanzada del CSP, creado utilizando las Claves de Firma de CSP.
- Los nombre distintivo y el número de serie únicos asignados por KeyOne CA. Esto es único en lo concerniente a la emisión de CSP.
- El certificado especifica un tiempo `valid from` que no precede al tiempo actual y un tiempo `valid until` que no precede al tiempo `valid from`.
- Los algoritmos/claves de firma utilizadas por KeyOne CA para firmar el certificado cumplen con el estándar de especificaciones de algoritmo [ALGO].
- Referencia a la Política de Certificado bajo el que el certificado se ha emitido.

Los requerimientos especificados en el Anexo 1 de [Eur99b] son los siguientes:

---

[95] *El script* `createpss.ws` *está ubicado en la carpeta de* scripts *de la ruta de acceso de instalación.*
[96] *El archivo de configuración* `root_ca_properties.txt` *está ubicado en la carpeta* `scripts` *de la ruta de acceso de instalación.*
[97] *El archivo de configuración* `subord_ca_properties.txt` *está ubicado en la carpeta* `scripts` *de la ruta de acceso de instalación.*

a) Una indicación de que el certificado está emitido como un certificado cualificado.

b) La identificación del proveedor-de-servicio-de-certificación y el estado en que está establecida.

c) El nombre del titular o el pseudónimo, que será identificado como tal.

d) Provisión para un atributo específico de un titular que se debe incluir si es relevante, dependiendo del propósito para el que intencionado el certificado.

e) Datos de verificación-de-firma que corresponden a datos de creación-de-firma data bajo el control del titular.

f) Una indicación del principio y fin del periodo de validez del certificado.

g) El código de identidad del certificado.

h) La firma electrónica avanzada del proveedor-de-servicio-de-certificación que lo emite.

i) Limitaciones ámbito del uso del certificado, si es aplicable.

j) Límite del valor de las transacciones para el que el certificado puede ser utilizado, si es aplicable.

Esta función es aplicable para los siguientes certificados:

- Certificados de titular cuya petición se recibe desde el Servicio de Registro.
- Certificados de Infraestructura[98], Control[99] y firma de QC/NQC, relacionados a los componentes KeyOne CA, KeyOne LRA, KeyOne TSA y KeyOne VA, para ser certificados por el Servicio de Generación de Certificados.

La función genera certificados con las características identificadas anteriormente, y está relacionada en las siguientes dos funcionalidades:

- Configuración del producto

  Para poder generar certificados que cumplieron estas características, es necesario configurar el producto KeyOne. Este proceso implica los siguientes cambios:

  - Configuración de las características del certificado generado, para certificados raíz y CSRs generadas por el *script* `createpss.ws`[100].
  - Configuración de las plantillas de certificación para certificados de titular y CSRs generados por el *script* `createpss.ws`.

---

[98] *Claves utilizadas por KeyOne VA, KeyOne CA y KeyOne TSA para procesos como la autenticación del subsistema, firma de registros de auditoría, transmisión de cifrado, …*
[99] *Claves utilizadas para personal de gestión o utilizando los componentes KeyOne VA, KeyOne CA y KeyOne TSA, y que pueden proporcionar autenticación, firma o confidencialidad para el personal interactuando con el sistema.*
[100] *El* script `createpss.ws` *está ubicado en la carpeta de* scripts *de la ruta de acceso de insolación.*



La modificación de archivos de configuración puede activar el comportamiento del producto para generar certificados que cumplen con las propiedades identificadas en esta función. Estas modificaciones de los archivos de configuración son **módulos de personalización de KeyOne** que son parte del **entorno del sistema**. El documento [CONFGUIDE] describe la personalización relacionada a la generación de certificados que cumplen con esta función.

- Generación de certificados

  Función relacionada a la generación de certificados, una vez que la función de la personalización ha finalizado.

Propiedades de certificado requeridas para esta función

La clave pública siempre se genera en un dispositivo criptográfico, tal y como se indica en el apéndice CPS de KeyOne 2.1, y se incluye en la Petición de Certificación.

Las firmas electrónicas avanzadas se basan en certificados cualificados (garantizados por la tecnología KeyOne), y se crean a través de un dispositivo de creación de firma seguro. El dispositivo de creación de firma seguro reúne los requerimientos expuestos en Anexo III de [Eur99b]. Tal y como se indica en el apéndice CPS de KeyOne 2.1, estos dispositivos se utilizarán en la arquitectura KeyOne.

Los datos de verificación de firma que corresponden a los datos de creación de firma, están contenidos en el certificado. La tecnología KeyOne incluye todos los datos necesarios para verificar la firma incluida en el certificado.

- Campo `SignatureAlgorithm`: Contiene el identificador del algoritmo criptográfico utilizado por la CA para firmar este certificado. Este campo contiene un identificador de algoritmo que se utiliza para identificar un algoritmo criptográfico, y parámetros opcionales relacionados al algoritmo. Para certificados raíz con claves DSA, en la tecnología KeyOne es obligatorio incluir los parámetros DSA en el certificado, y no es posible recuperarlos a través de jerarquía o de otros mecanismos (como especifica el estándar DSA). Para certificados no-raíz, es posible para indicar los parámetros DSA en la CSR, y por lo tanto, estos parámetros serán incluidos en el certificado.

- Campo `Signaturevalue`: Contiene una firma digital computada en ASN.1 DER codificación `tbsCertificate` (a ser firmado).

El método de generación del número de serie puede ser configurado en la plantilla de certificación relacionada al perfil relacionado con el certificado. La sección `serialNumber` de la pantalla de configuración del perfil especifica bien un método de generación secuencial (`sequential`) o un método de generación aleatorio (`timerandom`).

De forma predeterminada la aplicación KeyOne CA genera certificados con un nombre distintivo (que contiene el nombre del titular) que se especifica en el componente Autoridad de Registro, o en los archivos de propiedades que son únicos. El operador de registro en el componente Autoridad de Registro, o el administrador de KeyOne en el caso de una CSRs que se corresponde a un certificado de titular, verificar y la unicidad de estos nombres. Este procedimiento es requerido como se indica en el apéndice CPS de KeyOne 2.1. La tecnología KeyOne

garantiza la unicidad del número de serie generado por una Autoridad de Certificación.

Archivos de configuración que contienen las propiedades para certificados y CSRs

Algunas características de los certificados requeridos por esta función pueden ser configuradas en el archivo de propiedades de los componentes KeyOne. Para cada componente y servidor, un archivo de propiedades especifica las características para las claves y certificados para las entidades relacionadas. Este archivo será utilizado como un parámetro de entrada para el *script* que generarás las claves y los certificados.

- KeyOne CA

  El archivo `<type of entity>_ca_properties.txt`[101] indica las propiedades de las claves y certificados. El atributo `CN` contenido en la variable `subject` contiene el nombre de la entidad. Para certificados de SSL local, este `CN` contendrá el nombre del servidor o la IP relacionada a este servidor (otro nombre puede ser añadida en la variable `ssl_local_subjectAltNames` en este caso).

  La variable `<type of key>_serialNumber`[102] especifica el número de serie de los certificados o CSR.

  Las variables `subject` y `ssl_local_subject` (para certificado de SSL local) contienen el nombre distintivo relacionado al titular del certificado.

  La variable `<type of key>_duration`[103] especifica la validez de la clave (alternativamente, es posible utilizar la variable `<type of key>_NotAfter`[104] indicando el campo `notAfter` del certificado, y asumiendo el tiempo de generación del certificado para el campo `notBefore`).

  Para certificados de CA, la variable `<type of key>_keyAlgorithm`[105] especifica el algoritmo de clave. De forma predeterminada, este algoritmo corresponde al algoritmo de RSA (valor `rsaEncryption`). Es posible cambiar este valor para poder generar claves de DSA (en este caso, el valor para esta variable debe ser `id_dsa`).

---

[101] `<type of entity>` *indica el tipo de entidad que posee las claves (*`root_ca` *corresponde a una Autoridad de Certificación raíz,* `root_online` *corresponde a una Autoridad de Certificación online raíz,* `subord_ca` *corresponde a una Autoridad de Certificación subordinada, y* `subord_online` *corresponde a una Autoridad de Certificación online subordinada). Está ubicado en la carpeta de scripts de la ruta de acceso de instalación.*

[102] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRLs,* `ds` *para certificados* `de` *firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*

[103] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRLs,* `ds` *para certificados* `de` *firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*

[104] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves de firma de certificados y CRLs,* `ds` *para certificados* `de` *firma digital,* `de` *para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*

[105] *Donde* `<type of key>` *indica el tipo de clave:* `csrs` *para claves* `de` *firma de certificados y CRLs,* `ds` *para certificados,* `de` *firma digital, de para cifrado de datos,* `ssl_local` *para SSL local y* `ssl_online` *para SSL.*



El campo *<type of key>*_extensions.certificatePolicies[106] permite especificar si la extensión id-ce-certificatePolicies definida en [X.509] debe ser incluida en los certificados emitidos o no, y los valor de los identificadores. En esta variable, es posible indicar que el certificado ha sido emitido como un certificado cualificado.

La identificación del proveedor de servicio de certificado y el estado en que está establecido, está contenido en la variable subject (atributos DN) en caso de certificados raíz. Para certificados no-raíz, este campo será insertado por la aplicación KeyOne CA.

Para claves de máster i3D, el archivo db_master_properties.txt[107] indica las propiedades de las claves y de los certificados para una entidad de máster de i3D, si tiene un PSS separado del componente de CA. Como se indica en el apéndice CPS de KeyOne 2.1, las claves de CA se utilizarán como mecanismos i3D y el PSS de i3D relacionado al máster de la base de datos no se utilizará.

- KeyOne LRA

El archivo lra_properties.txt[108] indica las propiedades de las claves y de los certificados. El atributo CN contenido en la variable subject contiene el nombre de la entidad. Para certificados de SSL local, este CN debe contener el nombre del servidor o la IP relacionada a este servidor (otro nombre puede ser añadido en la variable ssl_local_subjectAltNames en este caso).

La variable *<type of key>*_serialNumber[109] especifica el número de serie del certificado o CSR.

Las variables subject y ssl_local_subject (para certificado de SSL local) contiene el nombre distintivo relacionado al titular del certificado.

La variable *<type of key>*_duration[110] especifica la validez de la clave (alternativamente, es posible utilizar la variable *<type of key>*_NotAfter[111] indicando el campo notAfter del certificado, y asumiendo el tiempo de generación del certificado para el campo notBefore).

El campo *<type of key>*_extensions.certificatePolicies[112] permite especificar si la extensión id-ce-certificatePolicies definida en [X.509] debe ser incluida en el certificado emitido o no, y los valor de los identificadores. En esta variable es posible indicar que el certificado ha sido emitido como un certificado cualificado.

La identificación del proveedor de servicio de certificado y el estado en el que se establece, está contenido en la variable subject (atributos de DN) para

---

[106] *Donde* <type of key> *indica el tipo de clave:* *csrs* *para claves de firma de certificados y CRLs,* ds *para certificados* de *firma digital, de para cifrado de datos,* *ssl_local* *para SSL local y* *ssl_online* *para SSL.*
[107] *Está ubicado en la carpeta de scripts de la ruta de acceso de instalación.*
[108] *Está ubicado en la carpeta de scripts de la ruta de acceso de instalación.*
[109] *Está ubicado en la carpeta de scripts de la ruta de acceso de instalación.*
[110] *Donde* <type of key> *indica el tipo de clave:* ds *para certificados* de *firma digital y* *ssl_local* *para SSL local.*
[111] *Donde* <type of key> *indica el tipo de clave:* ds *para certificados de firma digital,* de *para cifrado de datos y* *ssl_local* *para SSL local.*
[112] *Está ubicado en la carpeta de scripts de la ruta de acceso de instalación.*

certificados raíz. Para certificado no-raíz, este campo será insertado por la aplicación KeyOne CA.

- KeyOne TSA

 El archivo `tsa_properties.txt`[113] indican las propiedades de las claves y los certificados. El atributo `CN` contenido en la variable `subject` contiene el nombre de la entidad. Para certificados de SSL local, este `CN` contendrá el nombre del servidor o de la IP relacionada a este servidor (se puede añadir otro nombre en la variable `ssl_local_subjectAltNames` en este caso).

 La variable `<type of key>_serialNumber`[114] especifica el número de serie de los certificados o de la CSR.

 Las variables `subject` y `ssl_local_subject` (para certificado de SSL local) contiene el nombre distintivo relacionado al titular del certificado.

 La variable `<type of key>_duration`[115] especifica la validez de la clave (alternativamente es posible utilizar la variable `<type of key>_NotAfter`[116] indicando el campo `notAfter` del certificado, y asumiendo el tiempo de generación del certificado para el campo `notBefore`).

 El campo `<type of key>_extensions.certificatePolicies`[117] permite especificar si la extensión `id-ce-certificatePolicies` definida en [X.509] debe ser incluida en el certificado emitido o no, y los valor de los identificadores. En esta variable es posible indicar que el certificado ha sido emitido como un certificado cualificado.

 La identificación del proveedor de servicio de certificado y el estado en que se establece, está contenido en la variable `subject` (atributos DN) en caso de certificados raíz. Para certificados no-raíz, este campo será insertado por la aplicación KeyOne CA.

 Para las claves de máster de i3D el archivo `db_master_properties.txt`[118] indica las propiedades de las claves y de los certificados para una entidad de máster de i3D, si tiene un PSS separado del componente de CA. Tal y como se indica en el apéndice CPS de KeyOne 2.1, las claves de CA se utilizarán como mecanismo de i3D y el PSS de i3D relacionado al máster de la base de datos no se utilizará.

- KeyOne VA

 El archivo `keyoneva_keys.def`[119] indica las propiedades de las claves y de los certificados.

---

[113] *Está ubicado en la carpeta de scripts de la ruta de acceso de instalación.*
[114] *Está ubicado en la carpeta de scripts de la ruta de acceso de instalación.*
[115] *Donde `<type of key>` indica el tipo de clave: `ds` para certificados de firma digital, `de` para cifrado de datos y `ssl_local` para SSL local.*
[116] *Donde `<type of key>` indica el tipo de clave: `ds` para certificados de firma digital, `de` para cifrado de datos y `ssl_local` para SSL local.*
[117] *Donde `<type of key>` indica el tipo de clave: `ds` para certificados de firma digital, `de` para cifrado de datos y `ssl_local` para SSL local.*
[118] *Está ubicado en la carpeta de scripts de la ruta de acceso de instalación.*
[119] *Este archivo está ubicado en la carpeta de datos de la ruta de acceso de instalación.*



El atributo `CN` contenido en la variable `subject` contiene el nombre de la entidad.

La variable `subject` contiene el nombre distintivo relacionado al titular del certificado.

La variable `notAfter` indica el campo `notAfter` del certificado, y asumiendo el tiempo de generación del certificado para el campo `notBefore`).

El campo `template.certificatePolicies` permite especificar si la extensión `id-ce-certificatePolicies` definida en [X.509] debe ser incluida en le certificado o no, y el valor de los identificadores. En esta variable es posible indicar que el certificado ha sido emitido como un certificado cualificado.

La identificación del proveedor de servicio de certificado y el estado en que está establecido, están contenidos en la variable `subject` (atributos de DN) para certificados raíz. Para certificados no-raíz, este campo será insertado por la aplicación KeyOne CA.

Para claves de máster de i3D el archivo `db_master_properties.txt`[120] indica las propiedades de las claves y de los certificados para una entidad de máster de i3D, si tiene un PSS separado del componente de CA. Tal y como se indica en el apéndice CPS de KeyOne 2.1, las claves de CA se utilizarán como mecanismos de i3D y el PSS de i3D relacionado al máster de la base de datos no se utilizará.

En la fase de puesta en marcha, se crea el PSS relacionado a KeyOne CA, KeyOne LRA, KeyOne TSA y KeyOne VA. Para esto, se debe utilizar una de las utilidades en línea de comandos incluidas en la tecnología KeyOne. Esta utilidad se llama `createpss.ws`[121] y además del PSS, generará las claves privadas y opcionalmente los certificados dependiendo del tipo de CA.

Sobre las CSRs, a pesar de que se indica una validez en la CSR, cuando KeyOne CA genera el certificado relacionado a esta CSR, aplicará la política asociada, y comprobará que la validez especificada es compatible a la indicada en la CSR.

Plantillas de certificado restringiendo las propiedades para certificados

La plantilla de certificación se aplica a una petición de certificado antes de emitir el correspondiente certificado. Qué plantilla de certificación se aplica a una petición dada es una decisión que no se toma automáticamente. En cambio, las Autoridades de Registro que emiten los lotes de certificación procesados por KeyOne CA deben indicar qué plantilla de certificación debe ser aplicada a cada petición de lote. Una RA puede tener asociada cada petición a un nombre de plantilla de certificación específica en muchas maneras. La CA y las varias RAs debe estar de acuerdo sobre los nombre de la plantilla de certificación que se utilizan; esta decisión es comúnmente tomada durante la fase de puesta en marcha del software correspondiente.

Para CSRs procesadas del Servicio de Certificación, la plantilla de certificación a aplicar a la petición se solicitará en el proceso de certificación.

---

[120] *Está ubicado en la carpeta de scripts de la ruta de acceso de instalación.*
[121] *El script `createpss.ws` está ubicado en la carpeta de scripts de la ruta de acceso de instalación.*

En la plantilla de certificación, el campo `validityPeriod` es obligatorio y especifica el tiempo máximo de duración del certificado emitido así como la duración predeterminada si no se ha solicitado un tiempo de caducidad. Este campo es negociable, esto es, la petición de certificado puede proponer un valor para esto. Cuando se genera un certificado, su fecha de inicio de validez (campo `notBefore` del certificado) siempre se establecerá a la fecha actual. El campo `validityPeriod` de la plantilla de certificación se utilizará para calcular la fecha de caducidad (campo `notAfter`) como sigue:

- Si la petición de certificado no incluye la fecha de caducidad, se utiliza el resultado de añadir la duración especificada en el campo `validityPeriod` a la fecha actual.
- Si la petición de certificado incluye una fecha de caducidad y la fecha solicitada no es posterior que el resultado de añadir la duración especificada en el campo `validityPeriod` a la fecha actual, entonces se utiliza la fecha solicitada.
- Si la petición de certificado incluye una fecha de caducidad, pero la fecha solicitada es posterior al resultado de añadir la duración especificada en el campo `validityPeriod` a la fecha actual, entonces se utiliza esta segunda fecha.

El valor del campo `validityPeriod` debe ser especificado como un múltiplo de años, meses, días, horas, minutos o segundos. Escoja una de estas unidades de tiempo de la lista desplegable y entonces entre la cantidad de unidades en el campo de texto.

En la plantilla de certificación configurada desde la aplicación de administración de KeyOne CA, también es posible indicar la extensión `certificatePolicies`. El campo `certificatePolicies` permite especificar si la extensión `id-cecertificatePolicies` definida en [X.509] debe ser incluida en el certificado emitido o no, y el valor que debe tomar si está incluida.

Los algoritmos/calves de firma utilizados pueden ser configurados en la plantilla de certificación relacionada al perfil relacionado al certificado.

- La sección `signingAlgorithms` del pantalla de configuración del perfil puede especificar uno de los siguientes valores para los algoritmos de firma:
  - `sha1WithRsaSignature` (SHA1 con RSA)
  - `md5WithRsaSignature` (MD5 con RSA)
  - `md2WithRsaSignature` (MD2 con RSA)
  - `id_dsa_with_sha1` (SHA1 con DSA)
- La sección `publicKey.algorithm` de la pantalla de configuración del perfil puede especificar uno de los siguientes valores para la calve:
  - `rsaEncryption` (clave pública RSA)
  - `id_dsa` (clave pública DSA)

  Adicionalmente es posible indicar los parámetros de clave (`publickey.parameters`) y el tamaño de clave (`minBits` y `maxBits`).



FXT_XCG.1.6_QC - Generación de Certificación

Todos los QCs emitidos por el sistema KeyOne cumplen con [TS101862].

Esta función es aplicable a los titulares de los certificados cuya petición se recibe del servicio de registro.

La función genera certificados con las características definidas en [TS101862], y están implicados en las siguientes dos funcionalidades:

- Configuración del producto

  Para poder generar certificados que cumplen estas características, es necesario configurar el producto KeyOne. Este proceso implica la configuración de la plantilla de certificación para certificados de titular.

  Con la modificación de las plantillas de certificación es posible activar el comportamiento del producto para generar certificados que cumplen con las propiedades identificadas en esta función. Estas modificaciones de la plantilla de certificación pueden ser importadas desde los archivos de configuración, y por lo tanto son **módulos de personalización de KeyOne** que son parte del **entorno del sistema**. El documento [CONFGUIDE] describe la personalización relacionada a la generación de certificados que cumplen con esta función.

- Generación de certificados

  Función implicada en la generación de certificados, una vez que la función de personalización ha finalizado.

Propiedades de certificado requeridas por esta función

La clave pública se genera siempre en un dispositivo criptográfico, tal y como se indica en el apéndice CPS de KeyOne 2.1, y se incluye en la Petición de Certificación.

Las firmas electrónicas avanzadas están basadas are en certificados cualificados (garantizado por la tecnología KeyOne), y están creados por un dispositivo de creación de firma seguro. El dispositivo de creación de firma seguro cumple los requerimientos expuestos en el Anexo III de [Eur99b]. Como se indica en el apéndice CPS de KeyOne 2.1, estos dispositivos se utilizarán en la arquitectura de KeyOne.

Los datos de verificación de firma que corresponden a los datos de creación de firma, están contenidos en el certificado. La tecnología KeyOne incluye todos los datos necesarios para poder verificar la firma incluida en el certificado.

- Campo `SignatureAlgorithm`: Contiene el identificador del algoritmo criptográfico utilizado por la CA para firmar este certificado. Este campo contiene un identificador de algoritmo que se utiliza para identificar un algoritmo criptográfico, y parámetros opcionales relacionados al algoritmo. Para certificados raíz con claves DSA, en la tecnología KeyOne es obligatorio incluir los parámetros DSA en el certificado, y no es posible recuperarlas a través de la jerarquía u otros mecanismos (como especifica el estándar DSA). Para certificados no-raíz, es posible indicar en la CSR los parámetros de DSA, y por lo tanto estos parámetros se incluirán en el certificado.

- Campo `Signaturevalue`: Contiene la firma digital computada en el ASN.1 DER codificado `tbsCertificate` (que se debe firmar).

El método de generación del número de serie puede ser configurado en la plantilla de certificación relacionada al perfil relacionado al certificado. La sección `serialNumber` de la pantalla de configuración del perfil especifica bien un método de generación secuencial (`sequential`) o un método de generación aleatorio (`timerandom`).

De forma predeterminad la aplicación KeyOne CA genera certificados con un nombre distintivo (que contiene el nombre del titular) que se especifica en el componente Autoridad de Registro, o en los archivos de propiedades que son únicos. El operador de registro en el componente de la Autoridad de Registro, o el administrador KeyOne en el caso de las CSRs que no se corresponden a los certificados de titular, verifica la unicidad de estos nombres. Este procedimiento se requiere tal y como se indica en el apéndice CPS de KeyOne 2.1. La tecnología KeyOne garantiza la unicidad de los números de serie generados por una Autoridad de Certificación.

Plantillas de certificado que restringen las propiedades para certificados

Se aplica una plantilla de certificación a la petición de certificado antes de emitir el certificado correspondiente. Qué plantilla de certificación se aplica a una petición determinada es una decisión que se toma automáticamente. En cambio, la Autoridad de Registro que emite los lotes de certificación procesados por KeyOne CA debe indicar qué plantilla de certificación debe ser aplicada a cada petición de lote. Una RA puede tener asociada cada petición a un nombre de una plantilla de certificación específica de muchas maneras. La CA y las varias RAs debes estar de acuerdo en los nombres de la plantilla de certificación que se utilizan; esta decisión comúnmente se toma durante la fase de puesta en marcha del software correspondiente.

En la plantilla de certificación, el campo `validityPeriod` es obligatorio y especifica la duración máxima de los certificados emitidos al igual que la duración predeterminada si no se ha solicitado ninguna fecha de caducidad. Este campo es negociable, esto es, la petición de certificado puede proponer un campo para ello. Cuando se genera un certificado, su fecha de inicio de validez (campo `notBefore` del certificado) se establecerá en la fecha actual. El campo `validityPeriod` de la plantilla de certificación se utilizará para calcular la fecha de caducidad (campo `notAfter`) como sigue:

- Si la petición de certificado no incluye una fecha de caducidad, se utiliza el resultado de añadir la duración especificada en el campo `validityPeriod` a la fecha actual.

- Si la petición de certificado incluye una fecha de caducidad y la fecha solicitada no es posterior que el resultado de sumar el resultado de la duración especificada en el campo `validityPeriod` a la fecha actual, entonces se utiliza la fecha solicitada.

- Si la petición de certificado incluye una fecha de caducidad pero la fecha solicitada es posterior al resultado de sumar la duración especificada en el campo `validityPeriod` a la fecha actual, entonces se utilizan esta segunda fecha.



El valor del campo validityPeriod debe ser especificado como un múltiplo de años, meses, días, horas, minutos o segundos. Escoja una de estas unidades de tiempo de la lista desplegable y entonces entre la cantidad de unidades en el campo de texto.

En la plantilla de certificación configurada desde la aplicación de Administración de KeyOne CA, también es posible indicar la extensión certificatePolicies. El campo certificatePolicies permite especificar si la extensión id-cecertificatePolicies definida en [X.509] debe ser incluida en el certificado emitido o no, y el valor que debe tomar si está incluido. La indicación de que el certificado es un Certificado Cualificado se proporciona a través de la inclusión de id-etsi-qcs-QcCompliance OID en la extensión.

Los algoritmos/claves de firma utilizadas se pueden configurar en la plantilla de certificación relacionada al perfil relacionado el certificado.

- La sección signingAlgorithms de la pantalla de configuración del perfil puede especifica uno de los siguientes valores para los algoritmos de firma:
  - sha1WithRsaSignature (SHA1 con RSA)
  - md5WithRsaSignature (MD5 con RSA)
  - md2WithRsaSignature (MD2 con RSA)
  - id_dsa_with_sha1 (SHA1 con DSA)
- La sección publicKey.algorithm de la pantalla de configuración del perfil puede especificar uno de los siguientes valores para la clave:
  - rsaEncryption (clave publica RSA)
  - id_dsa (clave publica DSA)

  Adicionalmente, es posible indicar los parámetros de clave (publickey.parameters) y el tamaño de clave (minBits y maxBits).

El campo keyUsage permite especificar si la extensión id-ce-keyUsage definida en [X.509] debe estar ausente, presente o opcionalmente presente. En el caso del certificado cualificado esta extensión tendrá el valor nonRepudiation.

FXT_XCG.2.3 - Renovación de Certificación

El sistema KeyOne asegura que las Claves de Firma de QC/NQC se actualizan antes de su caducidad. Las claves públicas relacionadas (renovadas) proporcionan al menos el mismo nivel de confianza que cuando fueron distribuidas inicialmente.

Esto puede conseguirse al menos proporcionando al menos los siguientes certificados intermedios para probar la posesión de la nueva clave privada como sigue:

- Proporcionando un certificado de la anterior clave publica firmada con la nueva clave privada;
- Proporcionando un certificado de la nueva clave pública firmada con la anterior clave privada;

- Proporcionando el nuevo certificado auto-firmado (firmado con la nueva clave privada).

La renovación de la clave de firma de QC/NQC se consigue de acuerdo al procedimiento descrito en el apéndice CPS de KeyOne 2.1. El cumplimiento de este procedimiento asegura la realización de esta función.

El proceso de renovación consiste la ejecución del mismo mecanismo de seguridad que un proceso de certificación inicial, y consecuentemente esta función proporciona el mismo nivel de confianza que cuando se distribuyó inicialmente las claves de firma de QC/NQC.

En el proceso de renovación, se proporcionará (el mismo procedimiento que una certificación inicial) un certificado auto-firmado (firmado con la nueva clave privada).

FXT_XCG.2.4 - Renovación de Certificación

El sistema KeyOne proporciona un mecanismo para la regeneración de claves de claves de titular, que es tan seguro como la generación de certificado inicial.

La renovación (regeneración de las claves) de las claves de titular se consigue de acuerdo al procedimiento descrito en el apéndice CPS de KeyOne 2.1. El cumplimiento de este procedimiento asegura la realización de esta función.

El proceso de renovación consiste en la ejecución de los mismos mecanismos de seguridad que un proceso de certificación inicial, y consecuentemente esta función proporciona el mismo nivel de seguridad que cuando se generó el certificado inicial.

FXT_XGE – Seguridad de los Servicios Generales

FXT_XGE.1.1 – Seguridad de los Servicios Generales

Todos los mensajes creados por cualquier servicio básico:

- Están protegidos (ex. utilizando códigos de autenticación de mensaje, firmas digitales, etc.) utilizando las claves de infraestructura del servicio;
- Contiene un tiempo de mensaje, para indicar el tiempo en el que el remitente creó el mensaje;
- Incluye protección contra ataques de repetición (ex. utilizando *nonces*).

Los componentes KeyOne (KeyOne CA, KeyOne LRA y KeyOne VA) relacionados a los servicios básicos hacen cumplir la generación de evidencia de origen e integridad para peticiones y respuestas transmitidas en todo momento.

La evidencia del origen de los mensajes y la integridad está proporcionada por la generación de la firma digital de mensajes de peticiones y respuestas. Tanto el Lote KeyOne (comunicación entre KeyOne LRA y KeyOne CA) y los mensajes NDCCP (comunicación entre KeyOne VA y KeyOne CA) van firmados digitalmente.



Comunicación entre KeyOne VA y KeyOne CA

El componente KeyOne VA proporciona mensajería en tiempo real que implica un mecanismo de petición/respuesta. Una petición de estado vía Servicio de Estado de Revocación (componente KeyOne VA) consulta la Base de datos de Estado de Certificados y una respuesta de estado se genera y se devuelve vía Estado de Revocación.

KeyOne CertStatus Server es un módulo ubicado en el subsistema KeyOne CA que es responsable del servidor que consulta el estado del certificado desde el componente KeyOne VA. Este módulo consulta la base de datos de KeyOne CA y responde con información de revocación sobre esos certificados cuyo estado ha cambiado después de un cierto tiempo.

NDCCP (Near Domain Cert-status Coverage Protocol) es un protocolo propietario de Safelayer, que se utiliza en la comunicación entre el módulo Database Updater (en KeyOne VA) y un módulo CertStatus Server (en KeyOne CA). Esta comunicación sucede para mantener la base de datos de estado de la aplicación KeyOne VA actualizada.

Las características principales de este protocolo son:

- Utiliza HTTPS (HTTP con seguridad TLS/SSL) como mecanismo de transporte para los mensajes que se intercambian. Por lo tanto, existe un **canal de confianza** entre el Servicio de Gestión de Revocación (KeyOne CA) y el Servicio de Estado de Revocación (KeyOne VA).

  Por lo tanto, los mensajes NDCCP estarán incluidos dentro del cuerpo HTTP de los mensajes de petición/respuesta. Adicionalmente, estos mensajes usarán los siguientes valores en la cabecera *Content-Type*:

  - `application/x-safelayer-cert-status-req` para mensajes de petición NDCCP.
  - `application/x-safelayer-cert-status-resp` para mensajes de respuesta NDCCP.

- Los mensajes del protocolo están codificadas textualmente (ASCII).

El mensaje de petición NDCCP contiene un identificador de petición, y la respuesta relacionada generada por KeyOne CertStatus también contiene un campo indicando el identificador de la petición relacionada. Estos identificadores actúan como un ***nonce***, y por lo tanto estas peticiones y respuestas están protegidas de ataques de repetición.

Un **mensaje de petición NDCCP** tiene la siguiente sintaxis:

```
<sessionID>;<startFrom>;<timeRequest>

[UNSIGNED]

signature = <signature>
```

Donde:

`<sessionID>`: Identificador de la petición.

`<startFrom>`: Referencia de tiempo a considerar cuando se seleccionan los certificados cuyo estado ha cambiado. Sólo aquellos certificados cuyo estado ha cambiado después de este punto en el tiempo deben ser devueltos.

`<timeRequest>`: Tiempo en el que la petición se realizó.

`<signature>`: Firma digital de esa parte del mensaje de petición, que precede la etiqueta [UNSIGNED].

Un **mensaje de respuesta NDCCP** tiene la siguiente sintaxis:

```
<sessionID>;<nextDate>;<timeResponse>;<moreToCome>

<certInfo>

…..

[UNSIGNED]

signature = <signature>
```

Donde:

`<sessionID>`: Identificador de la petición asociada.

`<nextStartFrom>`: Valor que se debe incluir en el campo `<startFrom>` de la siguiente petición.

`<timeResponse>`: Fecha de la respuesta.

`<moreToCome>`: Etiqueta indicando si todos los certificados condicionados por la condición `request.<startFrom>` de la petición han sido incluidos en la respuesta. De lo contrario, otra petición con el valor `response.<nextStartFrom>` en su campo `response.<startFrom>` deben ser emitidos por el cliente.

- `<certInfo>`: Línea que contiene información sobre un certificado cuyo estado ha cambiado desde `request.<startFrom>`. Esta línea tiene la siguiente estructura:

  ```
  <sn>;<status>;<revreason>;<revdate>;<invdate>;<crtIss>;<holdCode>
  ```

  Donde:

  - `<sn>`: Número de series del certificado.
  - `<status>`: Estado actual del certificado.
  - `<revreason>`: Razón de revocación.
  - `<invdate>`
  - `<certIss>`
  - `<holdCode>`

Comunicación entre KeyOne CA y KeyOne LRA

La aplicación KeyOne LRA envía peticiones de certificación o revocación a la aplicación KeyOne CA. La aplicación KeyOne CA envía los certificados generados o



los resultados de revocación a la aplicación KeyOne LRA. El intercambio de estos datos se realiza utilizando el formato propietario: la estructura del lote KeyOne utilizando el protocolo HTTPS.

Estos son los estados del ciclo de vida del lote KeyOne:

- El lote lo crea la LRA. La LRA establece la información genérica del lote y añade las peticiones de certificación (o peticiones de revocación) al lote.
- Por razones de seguridad, la LRA firma el lote después de añadirle todos los datos. La firma de la LRA permite que la CA reconozca la LRA que envía el lote y se asegura que el lote no ha sido modificado durante la transmisión.
- La LRA envía el lote a la CA.
- La CA recibe el lote, valida su firma y realiza las operaciones solicitadas.
- La CA añade los resultados de las operaciones al lote y/o modifica los datos existentes. No se genera ningún lote nuevo. Los datos añadidos/modificados dependerán de las operaciones solicitadas. Para una petición de certificación, los certificados generados se añaden al lote. Para una petición de revocación, el resultado de la revocación se añade al lote. La cadena de certificación de la CA y las CRLs siempre se añaden al lote.
- Por razones de seguridad, la CA firma el lote después de añadirle todos los datos. La firma de CA permite que la LRA reconozca a la CA que envía el lote y se asegura que el lote no ha sido modificado durante la transmisión.
- La CA envía el lote a la LRA.
- La LRA recibe el lote, valida su firma y comprueba los resultados de las operaciones solicitadas.
- Si el lote contenido en la petición de certificación, la LRA extrae los certificados generados en la respuesta.

El ciclo de vida del lote KeyOne se puede resumir como sigue: KeyOne LRA genera el lote y le añade peticiones, KeyOne CA procesa estas peticiones y añade las respuestas al lote. Por lo tanto, la estructura de los lotes puede verse como datos añadidos por KeyOne LRA, datos añadidos por KeyOne CA e información genérica de lotes y extensiones de lotes.

Datos relacionados con KeyOne LRA

- Información genérica de KeyOne Batch

  La información genérica identifica el lote, el tipo de contenido y su estado actual. Los siguientes campos conforman la información genérica del lote:

  - `batchid`: Identificador de lote. Este campo identifica un lote entre otros lotes generados por una Autoridad de Registro.
  - `batchtype`: Tipo de lote. Este campo identifica el tipo de petición. Todas las peticiones en un lote deben tener el mismo tipo. Un lote puede ser:
    - `CR`: Un lote de certificación. Contiene peticiones de certificación.

- `RR`: Un lote de revocación. Contiene peticiones de revocación.
- `UR`: Un lote de actualización: Usado para intercambio de información entre RA y CA.

- `status`: Estado del lote. Corresponde más o menos al estado en que se encuentra el ciclo de vida del lote.

- Datos relacionados con KeyOne RA

  La Autoridad de Registro genera un lote y añade datos al lote que procesará la CA. Estos datos incluyen peticiones de certificación o revocación, a la vez que más datos con información que se deben intercambiar.

  Después de que se han añadido estos datos, la RA firma el lote, para garantizar que la CA lo reciba sin que sea modificado por un tercero.

  La información que la RA añade al lote es la siguiente:

  - Información general:
    - `timereq`: Fecha en que la RA generó el lote.
    - `rasubject`: Nombre distintivo de la RA que generó el lote.
    - `policiesReq`: Lista de políticas de certificación solicitadas. En un lote de certificación (CR), esta lista contiene todos los nombres de política de certificación que aparecen en la petición de certificación. Si el lote no es un lote de CR, este campo queda vacío.
  - CSRs

    La parte más importante de los datos añadidos por la RA al lote es la lista de peticiones.

    - `csrReportSeq`: Lista de peticiones. En un lote de CR habrá una petición de certificación. En un lote de RR habrá una petición revocación. En los otros tipos de lotes, este campo queda vacío.
  - Argumentos

    Los argumentos son datos adicionales enviados por la RA a la CA. Estos datos adicionales pueden ser información que la RA necesita recuperar una vez que la CA ha procesado el lote, u otro tipo de información que la CA puede necesitar. En lotes de UR, los argumentos son los datos intercambiados. Los campos son:

    - `scryptorGenericReq`: Datos que se envían a la CA.
  - Firma

    Después de añadir todos los datos al lote, la RA lo firma para asegurar que la CA recibe el lote sin que haya sido modificado por terceros. El único campo aquí es:

    - `rasignature`: Firma *detached* del lote generada por la RA.



Datos relacionados con KeyOne CA

El lote lo genera la Autoridad del Registro y y lo envía a la CA. La CA lee los datos del lote, lo procesa y añade los resultados al lote: certificados si era un lote de CR, resultados de revocación si el lote era de RR, o datos de información si el lote era de UR.

Al igual que la RA, la CA también firma el lote después de añadir los datos, para asegurar que la RA recibe el lote sin que haya sido modificado por terceros.

- Información

  Los campos de información identifican la CA que procesó el lote y cuando se procesó. Los siguientes campos conforman la información de la CA:

  - `timeresp`: Fecha en que la CA procesó el lote.
  - `casubject`: Nombre distintivo de la CA que procesó el lote.

- Certificados

  La parte más importante de los datos añadidos por la CA en el lote es la lista de respuestas. Se le llama **Certificados** porque es la respuesta a un lote de CR (una lista de certificados), pero contiene una lista de respuestas de revocación si el lote procesado es en lote de RR. Si es en lote de UR, normalmente este campo queda vacío.

  - `certReportSeq`: Lista de respuestas.

- Argumentos

  Los argumentos son datos adicionales enviados por la RA a la CA. La CA procesará estos datos y enviará otros datos como respuesta. Los datos que la CA envía pueden ser los mismos que se han recibido (sin que se hayan modificado) u otros datos generados como respuesta de datos recibidos. Los campos son:

  - `scryptorGenericGrant`: Datos que se enviarán a la RA.

- Cadena de certificación

  La CA añade su cadena de certificación completa al lote procesado: sus propios certificados, el certificado raíz (si no es un certificado raíz), y todos los certificados de las CAs subordinadas entre ese certificado y el certificado raíz de la CA (si los hay). Los siguientes campos forman parte de la cadena de certificación:

  - `keyCertSignCertificates`: Lista de certificados de firma de certificados. Los certificados combinados para firma de certificados y firma de CRL también se incluyen aquí. Si la CA no es un certificado de CA raíz, esta lista contiene sus propios certificados y los certificados de la CA subordinada entre este certificado y la CA raíz (si los hay). De lo contrario, si la CA es una CA raíz, esta lista queda vacía.
  - `keyCertSignRootCertificate`: Certificado de firma de certificados de la CA raíz. Si la CA es una CA raíz, este certificado es su propio certificado.

- `crlSignOnlyCertificates`: Lista de certificados de firma de CRL. Si la CA no es una CA raíz, esta lista contiene el certificado propio y todos los certificados entre las CAs subordinadas y la CA raíz (si los hay). De lo contrario, si la CA es una CA raíz, esta lista queda vacía. Esta lista también queda vacía si todas las CAs tienen certificados combinados para firma de certificados y firma de CRLs.

- `crlSignOnlyRootCertificate`: Certificados de firma de CRLs de la CA raíz. Si la CA es una CA raíz, este certificado es el certificado propio.

- `digitalSignatureCertificates`: Lista de certificados de firma digital. Si la CA no es un certificado de CA raíz, esta lista contiene el certificado propio y todos los certificados entre las CAs subordinadas y la CA raíz (si los hay). De lo contrario, si la CA es una CA raíz, esta lista queda vacía.

- `digitalSignatureRootCertificate`: Certificado de firma digital de la CA raíz. Si la CA es una CA raíz, este certificado es su propio certificado.

- CRLs

  La CA también añade sus CRLs al lote procesado para mantener la RA actualizada respecto a las CRLs. El campo es:

  - `crls`: Lista de CRLs.

- Firma

  Después de añadir todos los datos al lote, la CA los firma para asegurarse que la RA los recibe sin que el lote haya sido modificado por terceros. El único campo aquí es:

  - `casignature`: Firma *detached* de lote generada por la CA.

FXT_XR – Servicio de registro

FXT_XR.1.1 – Aplicación de certificado

Si la aplicación de certificado contiene información sensible del titular, la petición de certificado queda protegida antes de que sea enviado desde el Servicio de Registro al Servicio de Generación de Certificados y así garantizar la confidencialidad del mensaje. El sistema KeyOne asegura que esta funcionalidad se proporciona si se requiere.

Para cada servicio proporcionado por KeyOne LRA, debe conectarse al componente KeyOne CA.

KeyOne LRA genera una petición de certificación (lote de CR) o de revocación (lote de RR) a KeyOne CA utilizando el lote de petición firmado. KeyOne CA procesa el lote y envía las respuestas (certificados emitidos y resultados de revocación) a través de un lote firmado de respuesta. El contenido de la cabecera del mensaje entero está firmado por el remitente para permitir la integridad de la información.

Esta comunicación en este proceso de operación entre KeyOne LRA y KeyOne CA se establece utilizando SSL/TLS con autenticación de cliente. El protocolo SSL/TLS asegura la confidencialidad de los datos implicados en la comunicación.



FXT_XR.1.3 – Aplicación de certificado

El Servicio de Registro se configura para permitir la colección de suficientes datos del titular para satisfacer los requerimientos para QCs como se especifica en el Anexo I de [Eur99b].

Estos datos corresponden a la información relacionada con el certificado cualificado:

- Una indicación de que el certificado se emite como un certificado cualificado.
  - Esta indicación está configurada en la plantilla de certificación especificada en el componente KeyOne CA. La Autoridad de Registro añade información sobre si el certificado solicitado debe ser un QC en la petición, y entonces la Autoridad de Certificación aplicará esta política incorporando la extensión `certificatePolicies` con un valor indicando que el certificado es un QC.
- La identificación del proveedor del servicio de certificación y el Estado en que estableció.
  - Esta información la inserta la Autoridad de Certificación que genera el QC.
- El nombre del firmante o un pseudónimo, que se identificará como tal.
  - La aplicación de registro permite la posibilidad para indicar el nombre del firmante.
- Provisión para un atributo específico del firmante que se debe incluir, si es relevante, dependiendo del propósito para el que fue intencionado el certificado.
- Datos de verificación de firma que corresponde a los datos de creación de firma bajo el control del firmante.
  - La aplicación de certificación incorpora esta información en la QC (datos relacionados a los datos del algoritmo de firma).
- Una indicación del inicio y fin del periodo de validez del certificado.
  - Esta indicación está configurada en la plantilla de certificación especificada en el componente KeyOne CA. La Autoridad de Registro añade a la información de la petición que el certificado solicitado debe ser QC, y la Autoridad de Certificación aplicará esta política incorporando la validez indicada por la plantilla.
- El código de identidad del certificado.
  - La aplicación de certificación incorpora el número de serie único en el QC.
- La firma electrónica avanzada del proveedor de servicio de certificación que lo emite.
  - Las firmas electrónicas avanzadas están basadas en certificados cualificados (garantizados por la tecnología KeyOne), y están creados por un dispositivo de creación de firma de seguridad. El dispositivo de creación de firma de seguridad cumple los requerimientos explicados en el Anexo III

de [Eur99b]. Tal y como se indica en el apéndice CPS de KeyOne 2.1, estos dispositivos se utilizarán en la arquitectura KeyOne.

- Limitaciones en el ámbito de uso del certificado, si es aplicable.
- Límites sobre el valor de las transacciones para lo que se puede utilizar el certificado, si es aplicable.

FXT_XR.1.4 – Petición de Certificados

El sistema KeyOne provee un mecanismo para permitir la aprobación de peticiones de certificados, por un Oficial de Registro, antes de que éstas dejen el Servicio de Registro.

La aprobación de peticiones de certificados corresponde a la firma de las peticiones enviada por un operador de Autoridad de Registro. Puesto que todas las peticiones de certificado están firmadas digitalmente, esta aprobación significa que las peticiones de registro ofrecen el servicio de no-repudio. Todos los mensajes enviados desde autoridades de registro a KeyOne CA, se verifican y se almacenan en su Base de Datos. Puesto que la firma digital están dentro de los mensajes, la aprobación es mantenida también por la Autoridad de Certificación.

La clave usada para firmar las aprobaciones es la especificada como de firma digital en el componente KeyOne LRA[122]. La clave de firma y el certificado deben ser válidos y éstos deben de estar instalados en el almacén seguro privado de KeyOne LRA. El certificado de firma debe estar instalado en el componente KeyOne CA como de una Autoridad de Registro reconocida. El bloque de firma generado será insertado en el campo `signature` del lote que será enviado por HTTPS a KeyOne CA.

Esta función está relacionada con la funcionalidad de la firma de lotes in KeyOne LRA. El lote firmado generado por el componente KeyOne LRA es el siguiente:

- Información genérica del lote KeyOne

  La información genérica identifica el lote, el tipo de su contenido, y el estado actual. Los siguiente campos forman parte de la información genérica del lote:

  - `batchid`: Identificador del lote. Este campo identifica un lote entre todos los lotes generados por la Autoridad de Registro.
  - `batchtype`: Tipo de lote. Este campo identifica el tipo de peticiones de un lote. Todas las peticiones en un lote deben tener el mismo tipo. Un lote puede ser:
    - `CR`: Lote de Certificación. Contiene peticiones de certificación.
    - `RR`: Lote de Revocación . Contiene peticiones de revocación.
    - `UR`: Lote de Actualización. Usado para intercambiar información entre la RA y la CA.
  - `status`: Estado del lote. Corresponde más o menos a la fase del ciclo de vida donde se encuentra el lote.

[122] *Las propiedades para esta clave están especificadas en el fichero lra_properties.txt file que está ubicado en la carpeta scripts del directorio de instalación de KeyOne LRA.*



- Datos asociados a KeyOne RA

  La Autoridad de Registro genera el lote y añade datos al lote para que éste sea procesado por la CA. Estos datos incluyen peticiones de certificación or revocación, así como datos informativos para ser intercambiados.

  Después de que estos datos sean añadidos, la RA firma el lote, para garantizar que la CA lo recibe sin ninguna modificación por una tercera parte.

  La información que la RA añade al lote es la siguiente:

  - Información general:

    - `timereq`: Fecha y tiempo cuando el lote fue generado por la RA.
    - `rasubject`: Nombre Distinguido de la RA que generó el lote.
    - `policiesReq`: Lista de todas las políticas de certificación pedidas. En un lote de certificación (CR), esta lista contiene todos los nombres de políticas de certificación que aparecen en las peticiones de certificación. Si el lote no es un lote de CR, este campo está vacío.

  - CSRs

    La parte más importante de los datos añadidos por la RA al lote es la lista de peticiones.

    - `csrReportSeq`: Lista de peticiones. En un lote CR serán las peticiones de certificación. En un lote RR serán las peticiones de revocación. En los otros tipos de lote este campo estará vacío.

  - Parámetros

    Los parámetros son información adicional enviada por la RA a la CA. Estos datos adicionales pueden ser información que la RA necesita recuperar una vez que la CA ha procesado el lote, u otra información que la CA puede necesitar. En lotes UR, los parámetros son datos intercambiados. Los campos son:

    - `scryptorGenericReq`: datos a ser enviados a la CA.

  - Firma

    Después de añadir todos los datos al lote, la RA lo firma para asegurar que la CA recibe el lote sin que éste sea modificado por una tercera parte. El único campo es el siguiente:

    - **`rasignature`**: firma del lote generada por la RA.

FXT_XR.1.6 – Petición de Certificados

Las peticiones de certificados provenientes del Servicio de Registro están firmadas para proporcionar autenticación e integridad de datos, usando las claves de Control[123] o Infraestructura[124].

El operador de la Autoridad de Registro firma las peticiones generadas desde el componente KeyOne LRA. Puesto que todas las peticiones de certificado están firmadas digitalmente mediante la firma del lote (generada por la clave de control de KeyOne LRA) que contiene las peticiones de certificado, los servicios de autenticación e integridad de datos se proporcionan,

Todos los mensajes enviados desde autoridades de registro a KeyOne CA, se verifican y se almacenan en su base de datos. Puesto que la firma digital se encuentra dentro de los mensajes, la Autoridad de Certificación mantiene también la aprobación.

La clave usada para firmar la aprobación es la especificada como de firma digital en el componente KeyOne LRA[125]. La clave de firma y el certificado deben ser váldios y deben estar instalados en el almacén privado seguro de KeyOne LRA. Este certificado de firma debe estar instalado en el componente KeyOne CA como el de una Autoridad de Registro reconocida.

El bloque de firma generado se insertará en el campo `signature` del lote que se enviará por HTTPS a KeyOne CA.

Esta función está relacionada con la funcionalidad de firma de lotes en KeyOne LRA. El lote firmado generado por el componente KeyOne LRA en esta función es el siguiente:

- Información genérica del lote KeyOne

  La información genérica identifica el lote, el tipo de contenido y su estado actual. Los siguientes campos forman parte de la información genérica del lote:

  - `batchid`: Identificador del lote. Este campo identifica un lote entre todos los lotes generados por la Autoridad de Registro.
  - `batchtype`: Tipo de lote. Este campo identifica el tipo de peticiones del lote. Todas las peticiones en un lote deben tener el mismo tipo. Un lote puede ser:
    - `CR`: Lote de Certificación. Contiene peticiones de certificación.
    - `RR`: Lote de Revocación . Contiene peticiones de revocación.
    - `UR`: Lote de Actualización. Usado para intercambiar información entre la RA y la CA.

---

[123] Las Claves de Control son utilizadas por personal que gestiona o usa los componentes KeyOne VA, KeyOne CA y KeyOne TSA, y que pueden proveer autenticación, firma o confidencialidad para personal que interactúa con el sistema.
[124] Las Claves de Infraestructura son utilizadas por KeyOne VA, KeyOne CA y KeyOne TSApara procesos tales como autenticación de subsistemas, firma de registros de auditoría, datos transmitidos cifrados, …
[125] Las propiedades para esta clave se especifican en el fichero `lra_properties.txt` que está ubicado en la carpeta scripts del directorio de instalación de KeyOne LRA.



- `status:` Estado del lote. Corresponde más o menos a la fase del ciclo de vida donde se encuentra el lote.

- Datos asociados a KeyOne RA

  La Autoridad de Registro genera el lote y añade datos al lote para que éste sea procesado por la CA. Estos datos incluyen peticiones de certificación or revocación, así como datos informativos para ser intercambiados.

  Después de que estos datos sean añadidos, la RA firma el lote, para garantizar que la CA lo recibe sin ninguna modificación por una tercera parte.

  La información que la RA añade al lote es la siguiente:

  - Información general:

    - `timereq`: Fecha y tiempo cuando el lote fue generado por la RA.
    - `rasubject`: Nombre Distinguido de la RA que generó el lote.
    - `policiesReq`: Lista de todas las políticas de certificación pedidas. En un lote de certificación (CR), esta lista contiene todos los nombres de políticas de certificación que aparecen en las peticiones de certificación. Si el lote no es un lote de CR, este campo está vacío.

  - CSRs

    La parte más importante de los datos añadidos por la RA al lote es la lista de peticiones.

    - `csrReportSeq`: Lista de peticiones. En un lote CR serán las peticiones de certificación. En un lote RR serán las peticiones de revocación. En los otros tipos de lote este campo estará vacío.

  - Parámetros

    Los parámetros son información adicional enviada por la RA a la CA. Estos datos adicionales pueden ser información que la RA necesita recuperar una vez que la CA ha procesado el lote, u otra información que la CA puede necesitar. En lotes UR, los parámetros son datos intercambiados. Los campos son:

    - `scryptorGenericReq`: datos a ser enviados a la CA.

  - Firma

    Después de añadir todos los datos al lote, la RA lo firma para asegurar que la CA recibe el lote sin que éste sea modificado por una tercera parte. El único campo es el siguiente:

    - **`rasignature`**: firma del lote generada por la RA.

FXT_XR.2.1 – Gestión de Datos del Titular

El sistema KeyOne implementa mecanismos y controles de seguridad para proteger la privacidad y confidencialidad de la información del titular. Esta función asegura la

confidencialidad e integridad de los datos de usuario cuando éstos son transmitidos entre la Autoridad de Certificación y la Autoridad de Registro.

Respecto a la comunicación de la información del titular, los datos se protegen con privacidad y confidencialidad mediante el protocolo SSL/TLS. Toda la información del titular está cifrada utilizando la clave de sesión generada por el servidor KeyOne LRA, y previamente intercambiada usando el certificado de servidor SSL de KeyOne CA *online*. El protocolo SSL/TLS también asegura la integridad de los datos de usuario transmitidos.

FXT_XRM – Sistema de Gestión de Revocación de Certificados

FXT_XRM.1.2 – Petición de Cambio de Estado de Certificado

Todas las peticiones de suspensión, habilitación y revocación se autentican y validan apropiadamente.

Las peticiones de revocación, habilitación o suspensión pueden venir del servicio de registro KeyOne LRA (usualmente), o bien del servicio de certificación KeyOne CA. En ambos casos, hay un proceso de autenticación y validación.

Sólo los operadores autorizados pueden acceder a la función de cambio de estado de certificados ofrecida por KeyOne CA. Esta autorización implica una autenticación cuando el operador accede a los servicios de certificación.

El cumplimiendo del requisito FIA_UAU.2.1 asegura un mecanismo para autenticar exitosamente un operador antes de permitir que este usuario realice cualquier acción.

Si la petición de cambio de estado de certificación proviene del servicio de registro, entonces hay dos fases de autenticación en este proceso:

- Autenticación asociada al protocolo SSL/TLS establecido entre los componentes KeyOne LRA y Key CA. Entre el servidor KeyOne LRA y el servidor KeyOne CA *online*, se establece una conexión SSL/TLS con autenticación de cliente (la KeyOne CA *Online* actuando como servidor SSL/TLS).

  Para establecer esta conexión SSL/TLS con autenticación de cliente, se necesitan los siguientes dos tipos de certificados:

  - Certificado de servidor SSL de CA *Online*. Este certificado está presente en el Almacén Privado Seguro de KeyOne CA y será usado en la comunicación SSL con el componente KeyOne LRA.

  - Certificado de autenticación de la LRA. Este certificado está presente en el Almacén Privado Seguro de KeyOne LRA y será usado como certificado de cliente en la comunicación SSL con el componente KeyOne CA *online*.

  El proceso de autenticación de la LRA también implica la verificación de que el certificado de la LRA pertenece a una Autoridad de Registro reconocida. El administrador de la CA mantiene una lista de autoridades de registro que pueden comunicar con esta CA.



El uso de SSL/TLS en la comunicación entre KeyOne LRA y KeyOne CA, garantiza la integridad, autenticación del origen de los datos, privacidad y confidencialidad del mensaje de petición de certificado.

La comunicación SSL/TLS entre KeyOne LRA y KeyOne CA se explica en la sección `SSL/TLS communication between KeyOne LRA and KeyOne CA` del capítulo `Cryptographic Support` en el documento [FUNCSPEC].

- Autenticación asociada con el lote KeyOne. Todas las comunicaciones entre los componentes KeyOne LRA y KeyOne CA se realizan utilizando lotes KeyOne. El originador del lote siempre firma estos lotes, y previamente al proceso del lote, el receptor debe verificar la firma digital del lote. Adicionalmente, KeyOne CA verifica que la KeyOne LRA solicitante es una de las autoridades de registro reconocidas que están autorizadas a acceder a los servicios de certificación y revocación. El capítulo `Screen for configuring the recognized registration authorities in the KeyOne CA application` section of the `Certificate Revocation Management System` del documento [FUNCSPEC] explica la funcionalidad asociada al reconocimiento de RAs.

Adicionalmente a la autenticación del operador de registro, realizada por la Autoridad de Certificación, la Autoridad de Registro también autentica al sujeto que pide suspensión, habilitación o revocación. El apéndice CPS de KeyOne 2.1 contiene el procedimiento asociado a esta autenticación del sujeto realizada por el Operador de Registro.

FXT_XRM.1.3 – Petición de Cambio de Estado de Certificado

Una vez un certificado ha sido definitivamente revocado, el sistema KeyOne asegura que éste ya no puede ser habilitado (des-suspendido).

Cuando la revocación se vuelve efectiva (de acuerdo al requisito FPT_ITA.1.1), el componente KeyOne VA disemina el estado del certificado en las peticiones de estado de revocación. Una vez el certificado queda como revocado en la base de datos de KeyOne CA, éste no podrá ser de nuevo un certificado válido (porque sólo el estado de suspensión es un estado reversible, siendo la **revocación un estado irreversible**). El nucleo de la revocación en el servicio de certificación comprueba el estado de los certificados, y la aplicación sólo permite revocar los certificados suspendidos y válidos.

Esta función está asociada al núcleo del servicio de certificación que impide la reversibilidad del estado revocado, y también a la funcionalidad ofrecida por la aplicación que permite gestionar los cambios de estado de los certificados. Las secciones `Interface related to the changes of certificate status from the Registration Authority` y `Interface related to the changes of certificate status from the certification authority` del capítulo `Cryptographic Support` del documento [FUNCSPEC] explica esta funcionalidad.

FXT_XRM.1.4 – Petición de Cambio de Estado de Certificado

La revocación de certificados asociada a Claves de Firma de QC es sólo posible bajo como mínimo control dual.

Tal y como se describe en el apéndice CPS de KeyOne 2.1, las claves referenciadas anteriormente se generan y almacenan en un HSM (Modulo de Seguridad

Hardware), con control como mínimo de N personas de un total de M personas (N > 1).

Puesto que estas claves asimétricas son generadas por **componentes del entorno** (módulos criptográficos hardware), esta función está fuera del TOE (la comunicación entre el sistema KeyOne y los módulos criptográficos se realiza utilizando la especificación PKCS #11[126]). Sin embargo, aunque esta función sea responsabilidad del entorno, la tecnología KeyOne debe adaptarse a este entorno.

Esta configuración consiste en una configuración del proceso de generación del PSS y la ejecución de la aplicación KeyOne:

- Proceso de generación del PSS (esquema N de M, con un control mínimo de N personas, de un total de M personas, N > 1).

  Si se necesitan N tarjetas para acceder a las claves protegidas por el conjunto de tarjetas de operadores (OCS – *Operator Card Set*), se debe ejecutar la aplicación `with-nfast`[127] y el PSS se debe generar utilizando el parámetro `uri` en la herramienta de línea de comandos `createpss.ws`.

  - Windows: `c:\nfast\bin\with-nfast -t createpss.ws -from <properties_file> -uri "sfly:///pkcs11/interface.ws?p11Path=c:/nfast/toolkits/pkcs11/cknfast.dll"`

- Ejecución de la aplicación KeyOne (esquema N de M, con un control mínimo de N personas, de un total de M personas, N > 1).

  En las aplicaciones KeyOne que arrancan mediante el fichero `start<…>.bat`, es necesario modificar el fichero `start<…>.bat` para ejecutar la aplicación mediante el programa `with-nfast`[128].

  - Windows (ejemplo del fichero `start_nodb.bat` en la aplicación KeyOne CA): `start c:\nfast\bin\with-nfast -t keyoneca.exe -server_url" https://localhost:8081" -configfile "./config_ca.ws" -nodb`

  En otras aplicaciones, la aplicación KeyOne debe ser ejecutada mediante la aplicación `with-nfast`[129].

  - Windows: `c:\nfast\bin\with-nfast -t` *`<línea de comando de la aplicación KeyOne>`*

FXT_XRM.1.6 – Petición de Cambio de Estado de Certificado

La base de datos de Estado de Certificado se actualiza inmediatamente después de la finalización del procesamiento de una petición/informe (Rauth).

Respecto a las revocaciones provenientes del componente KeyOne CA, una vez la petición de revocación se efectúa, se actualiza automáticamente la base de datos de la CA.

---

[126] *La librería PKCS #11usada es la del fabricante del HSM.*
[127] *Esta aplicación es suministrada por el fabricante del HSM (Ncipher).*
[128] *Programa suministrado por el fabricante del HSM (Ncipher).*
[129] *Esta aplicación está suministrada por el fabricante del HSM (Ncipher).*



Respecto a las revocaciones provenientes del componente KeyOne LRA, éstas asimismo se actualizan automáticamente en la base de datos de KeyOne CA. Puesto que los componentes KeyOne LRA y KeyOne CA son procesos *online*, las peticiones provenientes de la Autoridad de Registro llegan a un servicio de certificación en tiempo real. Una vez la petición *online* llega al servicio de certificación, ésta se procesa y se actualiza la base de datos de la CA en tiempo real.

Esta función está relacionada con el núcleo del servicio de certificación que inmediatamente actualiza la base de datos de Estado de Certificados, y también con la funcionalidad ofrecida por la aplicación que permite gestionar los cambios de estado de certificados. Las secciones `Interface related to the changes of certificate status from the Registration Authority` y `Interface related to the changes of certificate status from the certification authority` del capítulo `Cryptographic Support` del documento [FUNCSPEC] explica esta funcionalidad.

FXT_XRM.2.2 – Petición de Cambio de Estado de Certificado

En el caso de uso de Mensajes Periódicos, el sistema KeyOne soporta los siguientes requisitos:

- En el caso de un repositorio de estados *offline* (como por ejemplo CRL acesible mediante directorios) el Servicio de Estado de Revocación se actualiza como mínimo diariamente.
- En el caso de un repositorio de estados *online* (como por ejemplo un servidor OCSP) el Servicio de Estado de Revocación se actualiza cuando ocurre el cambio de estado, y adicionalmente como mínimo una vez al día.
- Cada mensaje de actualización incluye el nombre y la firma digital del emisor del mensaje, y el tiempo de cambio de estado.
- El mensaje indica qué certificados se revocan/suspenden.
- Para cada certificado en la lista, en el mensaje se prevee de su número de serie y una razón del cambio de estado.

El uso de Mensajes Periódicos implica que se envían mensajes de actualización (como por ejemplo CRLs/ARLs) desde el Sistema de Gestión de Revocación hacia el Servicio de Estado de Revocación.

En el sistema KeyOne, la arquitectura corresponde a un servicio *online*, donde las partes confiables se comunican con el Servicio de Estado de Revocación, y proveen de detalles del certificado(s) de los cuales se requiere su estado. El Servicio de Estado de Revocación *online*, en el caso de uso de mensajes en tiempo real, hace una consulta a la base de datos de Estado de Certificados para recuperar el estado actual del certificado solicitado, y en el caso de uso de mensajes periódicos consulta en sus registros internos, los cuales han sido actualizados por el último mensaje periódico. De esta manera se crea una respuesta y se envía la parte confiable indicando el estado de los certificado(s) solicitados.

El sistema KeyOne corresponde a un servicio online que utiliza mensajes periódicos.

El Servidor KeyOne CertStatus es un módulo ubicado en el subsisteme KeyOne CA que es responsable de responder peticiones de estado de certificados provenientes

del componente KeyOne VA. Este módulo consulta la base de datos de KeyOne CA y responde información de revocación sobre los certificados cuyo estado ha cambiado después de un instante de tiempo determinado.

El tiempo de sincronización entre KeyOne CertStatus y KeyOne VA puede ser configurado para mantener siempre actualizado KeyOne VA. La aplicación de administración de KeyOne VA permite configurar el tiempo de sincronización. El apéndice CPS de KeyOne 2.1 especifica una recomendación para el período de tiempo entre dos actualizaciones de la base de datos, y el tiempo máximo dedicado a una actualización. La funcionalidad que ejecuta esta configuración recibe como entrada los valores para los campos de configuración `Update frecuency (sec.)` y `Update timeout (sec.)`. Los datos de configuración son accesibles desde la configuración del módulo `certstatusserver` module de la aplicación de Administración de KeyOne VA.

NDCCP (*Near Domain Cert-status Coverage Protocol*) es un protocolo propietario de Safelayer, que se utiliza en la comunicación entre el módulo `Database Updater` (en KeyOne VA) y el módulo `Cert-status Server` module (in KeyOne CA). Esta comunicación tiene lugar para mantener actualizada la base de datos de estados de la aplicación KeyOne VA.

Las principales características de este protocolo son:

- Usa HTTPS (HTTP securizado con TLS/SSL) como mecanismo de transporte para los mensajes intercambiados. Por tanto, existe un canal de confianza entre el Servicio de Gestión de Revocación (KeyOne CA) y el Servicio de Estado de Revocación (KeyOne VA).

  Por tanto, los mensajes NDCCP estarán incluidos dentro de los cuerpos de los mensajes de petición/respuesta HTTP. Adicionalmente, estos mensajes usarán los siguientes valores para las cabeceras Content-Type:

  - `application/x-safelayer-cert-status-req` para mensajes de petición NDCCP.
  - `application/x-safelayer-cert-status-resp` para mensajes de respuesta NDCCP.

- Los mensajes del protocolo están codificados en texto (ASCII).

El mensaje de petición NDCCP contiene un identificador de petición, y la respuesta asociada generada por KeyOne CertStatus también contiene un campo indicando el identificador de la petición con la que está relacionada. Estos identificadores actúan como un *nonce*, y por tanto estas peticiones y respuestas están protegidas de ataques de *reply*.

La petición contiene el tiempo en el que se generó el mensaje, la firma y el nombre del firmante (nombre distinguido del campo `subject` contenido en el certificado del firmante).

Un mensaje de petición NDCCP tiene la siguiente sintaxis:

```
<sessionID>;<startFrom>;<timeRequest>

[UNSIGNED]

signature = <signature>
```



Donde:

<*sessionID*>: Identificador de petición.

<*startFrom*>: Referencia de tiempo a considerar en la selección de certificados cuyo estado ha cambiado. Sólo aquellos certificados cuyo estado ha cambiado después de este instante deberían ser incluidos en la respuesta.

<*timeRequest*>: Tiempo en el que la petición se ejecuta.

<*signature*>: Firma digital de la parte del mensaje de petición que precede la etiqueta [UNSIGNED].

El mensaje de respuesta NDCCP tiene la siguiente sintaxis:

```
<sessionID>;<nextDate>;<timeResponse>; <moreToCome>

<certInfo>

…..

[UNSIGNED]

signature = <signature>
```

Donde:

<*sessionID*>: Identificador de la petición asociada.

<*nextStartFrom*>: Valor para incluir en el campo <*startFrom*> de la próxima petición.

<*timeResponse*>: Tiempo de la respuesta.

<*moreToCome*>: Marca indicando si todos los certificados que se corresponden con la condición *request.<startFrom>* han sido incluidos en la respuesta. En el caso de que no, otra petición con el valor response.<*nextStartFrom*> en su campo response.<*startFrom*> debería ser emitida por el cliente.

- <*certInfo*>: Línea conteniendo información sobre el certificado cuyo estado ha cambiado desde request.<*startFrom*>. Esta línea tiene la siguiente estructura:

  ```
  <sn>;<status>;<revreason>;<revdate>;<invdate>;<crtIss>;<holdCode>
  ```

  Donde:

  - <*sn*>: Número de Serie del certificado.
  - <*status*>: Estado actual del certificado.
  - <*revreason*>: Razón de revocation.
  - <*invdate*>
  - <*certIss*>
  - <*holdCode*>



El mensaje indica qué certificados han sido revocados/suspendidos mediante el campo *<sn>* (contenido en el campo *<certInfo>*). El Servicio de Estado de Revocación (KeyOne VA) solicita estados de certificados y el módulo KeyOne CertStatus consulta la base de datos de KeyOne CA (campo `status` de la tabla `cert_ca`) y responde proveiendo el estado actual de los certificados incluidos en la respuesta NDCCP (campo `certInfo.status` de la respuesta). Puesto que el módulo KeyOne CertStatus obtiene información de estado de revocación de la base de datos de KeyOne CA, éste provee el estado actual de los certificados.

FXT_XRS – Servicio de Estado de Revocación de Certificados

FXT_XRS.1.1 – Datos de Estado de Revocación

Los Mensajes Periódicos provistos a este servicio llegan desde los Servicios de Gestión de Revocación confiables.

La confianza de los Servicios de Gestión de Revocación se basa en la certificación del Servicio de Estado de Revocación (componente KeyOne VA) por una Autoridad de Certificación confiable. Para asegurar este requisito, el certificado de firma OCSP (certificado con el valor `OCSPSigning` en la extensión `extendedKeyUsage`) debe estar certificado por una Autoridad de Certificación de confianza para las entidades que solicitan servicios de validación *online*. De esta manera, el Servicio de Estado de Revocación estará mantenido en el mismo dominio de confianza que la Autoridad de Certificación.

El apéndice CPS de KeyOne 2.1 especifica un entorno de infraestructura que requiere la certificación de las VAs (certificados de firma OCSP) por una Autoridad de Certificación de dominio confiable. En este caso, is necesario configurar el componente KeyOne VA para generar certificados de firma OCSP de acuerdo con este requisito. El comportamiento por defecto del producto KeyOne cumple con este requisito (la variable `DEFAULT-OCSP_SIGNING_CERT_DEF.isRoot`[130] contiene un valor de `0`).

Además de la certificación del Servicio de Estado de Revocación por una CA de confianza, existe un reconocimiento mútuo entre la Autoridad de Certificación (KeyOne CA) y la Autoridad de Validación (KeyOne VA):

- El Servicio de Estado de Revocación (VA) debe ser aprobado para realizar peticiones en la CA donde la VA enviará mensajes periódicos para obtener información del estado de certificados. La sección `Configuration in the KeyOne CA of the list of recognized VAs` del capítulo `Certificate Revocation Status Service` en el documento [FUNCSPEC], especifica todos los detalles sobre el reconocimiento de VAs por Autoridades de Certificación.
- La Autoridad de Certificación a la que la VA enviará mensajes periódicos para obtener información del estado de los certificados, debe ser aprobada y configurada en el entorno de la VA (KeyOne VA). La sección `Configuration in the KeyOne VA of the CA (CertStatus Server) to request` del capítulo `Certificate Revocation Status Service` chapter en el documento

[130] *Esta variable está contenida en el fichero* `data/keyoneva_keys.def` *en e directorio de instalación del producto KeyOne VA.*



[FUNCSPEC], especifica todos los detalles sobre el reconocimiento de CAs por Autoridades de Validación.

FXT_XRS.1.2 – Datos de Estado de Revocación

Cuando el sistema KeyOne provee un servicio de estado de revocación *online*, valida la integridad y autenticación de los mensajes periódicos enviados a éste.

El sistema KeyOne corresponde a un servicio *online* con mensajes periódicos.

El Servidor KeyOne CertStatus es un módulo ubicado en el subsisteme KeyOne CA que es responsable de responder peticiones de estado de certificados provenientes del componente KeyOne VA. Este módulo consulta la base de datos de KeyOne CA y responde información de revocación sobre los certificados cuyo estado ha cambiado después de un instante de tiempo determinado.

En este caso, los mensajes periódicos corresponden con mensajes NDCCP intercambiados entre los servidores KeyOne CA y KeyOne VA.

NDCCP (*Near Domain Cert-status Coverage Protocol*) es un protocolo propietario de Safelayer, que se utiliza en la comunicación entre el módulo `Database Updater` (en KeyOne VA) y el módulo `Cert-status Server` module (in KeyOne CA). Esta comunicación tiene lugar para mantener actualizada la base de datos de estados de la aplicación KeyOne VA.

Las principales características de este protocolo son:

- Usa HTTPS (HTTP securizado con TLS/SSL) como mecanismo de transporte para los mensajes intercambiados. Por tanto, existe un canal de confianza entre el Servicio de Gestión de Revocación (KeyOne CA) y el Servicio de Estado de Revocación (KeyOne VA).

  Por tanto, los mensajes NDCCP estarán incluidos dentro de los cuerpos de los mensajes de petición/respuesta HTTP. Adicionalmente, estos mensajes usarán los siguientes valores para las cabeceras Content-Type:

  - `application/x-safelayer-cert-status-req` para mensajes de petición NDCCP.
  - `application/x-safelayer-cert-status-resp` para mensajes de respuesta NDCCP.
- Los mensajes del protocolo están codificados en texto (ASCII).

Puesto que los mensajes NDCCP (peticiones y respuestas) están firmados digitalmente, esta comunicación provee de los servicios de seguridad de integridad y autenticación.

Un mensaje de petición NDCCP tiene la siguiente sintaxis:

```
<sessionID>;<startFrom>;<timeRequest>

[UNSIGNED]

signature = <signature>
```

Donde:

<*sessionID*>: Identificador de petición.

<*startFrom*>: Referencia de tiempo a considerar en la selección de certificados cuyo estado ha cambiado. Sólo aquellos certificados cuyo estado ha cambiado después de este instante deberían ser incluidos en la respuesta.

<*timeRequest*>: Tiempo en el que la petición se ejecuta.

<*signature*>: Firma digital de la parte del mensaje de petición que precede la etiqueta [UNSIGNED].

El mensaje de respuesta NDCCP tiene la siguiente sintaxis:

```
<sessionID>;<nextDate>;<timeResponse>; <moreToCome>

<certInfo>

…..

[UNSIGNED]

signature = <signature>
```

Donde:

<*sessionID*>: Identificador de la petición asociada.

<*nextStartFrom*>: Valor a incluir en el campo <*startFrom*> de la próxima petición.

<*timeResponse*>: Tiempo de la respuesta.

<*moreToCome*>: Marca indicando si todos los certificados que se corresponden con la condición *request.<startFrom>* han sido incluidos en la respuesta. En el caso de que no, otra petición con el valor response.<*nextStartFrom*> en su campo response.<*startFrom*> debería ser emitida por el cliente.

- <*certInfo*>: Línea conteniendo información sobre el certificado cuyo estado ha cambiado desde request.<*startFrom*>. Esta línea tiene la siguiente estructura:

  <sn>;<status>;<revreason>;<revdate>;<invdate>;<crtIss>;<holdCode>

  Donde:

  - <*sn*>: Número de serie del certificado.
  - <*status*>: Estado actual del certificado.
  - <*revreason*>: Razón de revocación.
  - <*invdate*>
  - <*certIss*>
  - <*holdCode*>



FXT_XRS.2.1 – Petición/Respuesta de Estado

Todas las respuestas de estado de certificados provenientes de un Servicio de Estado de Revocación, están firmadas digitalmente por el Servicio de Estado de Revocación usando su clave de infraestructura[131].

El mensaje de respuesta contiene el tiempo en el que el Servicio de Estado de Revocación/Emisor firmó la respuesta.

Puesto que el servidor KeyOne VA genera mensajes de respuesta OCSP de acuerdo con la especificación [RFC2560], todos los campos obligatorios de este mensaje se incluyen en la respuesta OCSP generada. El campo `BasicOCSPResponse.signature` es información obligatoria definida por la RFC 2560, y éste contiene la firma digital de la respuesta de estado de certificados.

Los algoritmos/claves de firma utilizados por la respuesta de estado cumplen con [ALGO].

Por defecto el servidor KeyOne VA utiliza el algoritmo RSA con SHA1 para firmar respuestas OCSP para entidades solicitantes del estado de certificados. Estos algoritmos están incluidos en la lista de claves y algoritmos especificados en el estándar de especificaciones de algoritmos [ALGO]. Consecuentemente, el comportamiento por defecto del producto KeyOne cumple con este requisito (la variable `OCSP_SIGNING_KEY_DEF.keyAlgorithm`[132] contiene un valor de `rsaEncryption`).

FXT_XRS.2.4 – Petición/Respuesta de Estado

El mensaje de respuesta contiene el tiempo en el que el Servicio de Estado de Revocación/Emisor firmó la respuesta.

Puesto que el servidor KeyOne VA genera mensajes de respuesta OCSP de acuerdo con la especificación [RFC2560], todos los campos obligatorios de este mensaje se incluyen en la respuesta OCSP generada. El campo `BasicOCSPResponse.tbsResponseData.producedAt` es información obligatoria definida por la RFC 2560, y éste indica el tiempo en el que el emisor firma la respuesta. Cuando el servidor KeyOne VA genera la respuesta OCSP, éste incluye este tiempo en el campo `BasicOCSPResponse.tbsResponseData.producedAt` de la estructura.

FXT_XTS – Servicio de Sellado de Tiempo

FXT_XTS.3.1 – Generación de Sellos de Tiempo

El número de serie utilizado dentro del TST es único para cada TST emitido por una TSA determinada. Esta propiedad es preservada incluso después de una posible interrupción (por ejemplo una caída) del servicio.

---

[131] *Las claves de Infraestructura se utilizan por KeyOne VA, KeyOne CA y KeyOne TSA para procesar por ejemplo autenticación de subsistemas, firma de registros de auditoría, datos cifrados transmitidos, …*

[132] *Esta variable está contenida en el fichero data/keyoneva_keys.def del directorio de instalación del producto KeyOne VA.*

Puesto que el servidor KeyOne TSA genera una estructura TST (*Time Stamp Token*) de acuerdo con la especificación [RFC3161], todos los campos obligatorios de este mensaje se incluyen en las estructuras TST generadas. El campo `TSTInfo.serialNumber` es información obligatoria definida por la RFC 3161, y éste contiene un número de serie generado aleatoriamente para cada nuevo *token* de sello de tiempo generado.

FXT_XTS.3.3 – Generación de Sellos de Tiempo

Se incluye una indicación de la política bajo la cual el TST fue generado.

Puesto que el servidor de KeyOne TSA genera la estructura TST (*Time Stamp Token*) de acuerdo con la especificación [RFC3161], todos los campos obligatorios de este mensaje se incluyen en las estructuras TST generadas. El campo `TSTInfo.policy` es información obligatoria definida por la RFC 3161, y éste contien un parámetro de configuración indicando la política a aplicar.

La política se incluye en la variable `tsa_policy` del fichero de configuración `config_tsa_server_miscoptions.ws`[133].

Cuando KeyOne TSA arranca, el servidor comprueba que la variable `tsa_policy` contiene un OID especificando una política de TSA correcta.

FXT_XTS.4.5 – Time-Stamp Token (TST) Computation

La TSA asegura que las respuestas TST contienen los mismos datos que fueron enviados en las peticiones.

Puesto que el servidor KeyOne TSA implementa el protocolo TSP (*Time Stamp Protocol*) de acuerdo con la especificación [RFC3161], los datos a los que se ha aplicado el hash recibidos in la petición TSP (campo `timeStampReq.messageImprint`), son los mismos que los datos incluidos en la respuesta TSP (campo `tstInfo.messageImprint`).

FXT_XTS.4.6 – Cálculo del Token de Sello de Tiempo (TST)

Los algoritmos/claves de firma utilizados por la TSA, en el caso de que sea aplicable, cumplen los requisitos criptográficos especificados en [ALGO].

Por defecto el servidor de KeyOne TSA utiliza el algoritmo RSA con SHA1 para firmar TSTs para entidades que solicitan servicios de sellado de tiempo. Estos algoritmos están incluidos en la lista de algoritmos y claves especificados en el estándar de especificaciones de algoritmo [ALGO]. Esta función implica la configuración del fichero adecuado donde se especifican las características de la clave de firma de la TSA. En este caso, se deben de indicar los algoritmos especificados en [ALGO]. El apéndice CPS de KeyOne 2.1 explica las líneas directivas para cumplir con este requisito. Por defecto la configuración inicial del producto cumple con este requisito.

[133] *Este fichero de configuración está ubicado en el directorio* `config` *de la carpeta de instalación de KeyOne TSA.*



FXT_XSP – Servicio de Provisión de Dispositivo del Titular

FXT_XSP.2.1 – Provisión de SCDev

En el caso de que sea aplicable, el CSP asegura mediante la configuración apropiada del sistema KeyOne, que el SCDev sea distribuido a los titulares deseados y autenticados.

En el sistema KeyOne el Componente de Registro KeyOne LRA consiste en un esquema de registro cara a cara. Cuando el usuario se registra (presencia del titular), éste se autentica y entonces se generan las claves en el dispositivo SCDev.

La arquitectura KeyOne y el esquema de registro cara a cara aseguran que el SCDev es distribuido a los titulares deseados y autenticados. El procedimiento de registro se describe en el apéndice CPS de KeyOne 2.1.

Puesto que la protección y los mecanismos de seguridad asociados a la distribución segura del SCDev, están basados en la arquitectura KeyOne, entonces el cumplimiento de esta función está basado en un componente externo.

FXT_XSP.3.2 – Creación & Distribución de Datos de Activación

El sistema KeyOne asegura que el personal del CSP no puede en ningún momento hacer mal uso del SCDev.

El en el sistema KeyOne el componente de Registro KeyOne LRA consiste en un esquema de registro cara a cara. Cuando un usuario se registra (presencia del titular), el/ella es autenticado y se generan las claves en el dispositivo SCDev.

La arquitectura KeyOne y el esquema de registro cara a cara aseguran que el personal del CSP no puede en ningún momento hacer mal uso del SCDev. El procedimiento de registro se describe en el apéndice CPS de KeyOne 2.1.

Puesto que la protección y los mecanismos de seguridad asociados a la distribución segura del SCDev están basados en la arquitectura KeyOne, el cumplimiento de esta función se basa en un componente externo, y la información de entrada, salida y errores de esta función no se describe en este documento.

Tabla de asociación entre requisitos funcionales y funciones de seguridad

Esta sección incluye una tabla de asociación entre los requisitos funcionales de seguridad del TOE incluidos en esta Declaración de Seguridad y las funciones de seguridad del TOE especificadas en el documento [FUNCSPEC].

Requisito Funcional	*Función de Seguridad*
FAU_GEN.1.1	FAU_GEN.1.1
FAU_GEN.1.2	FAU_GEN.1.2
FAU_GEN.2.1	FAU_GEN.1.2
FAU_SAR.1.1	FAU_SAR.1.1

FAU_SAR.1.2	FAU_SAR.1.2
FAU_SAR.3.1	FAU_SAR.3.1
FAU_STG.1.1	FAU_STG.1.1
FAU_STG.1.2_1	FAU_STG.1.2_1
FAU_STG.1.2_2	FAU_STG.1.2_2
FCS_CKM.1.1_1	FCS_CKM.1.1_1
FCS_CKM.1.1_2	FXT_XKM.1.7
FCS_CKM.2.1	FCS_CKM.2.1
FCS_CKM.3.1	FCS_CKM.3.1
FCS_COP.1.1_1	FCS_COP.1.1_1
FCS_COP.1.1_2	FCS_COP.1.1_1
FCS_COP.1.1_3	FCS_COP.1.1_1
FCS_COP.1.1_4	FCS_COP.1.1_1
FCS_COP.1.1_5	FCS_COP.1.1_1
FIA_UID.1.1	FIA_UID.1.1
FIA_UID.1.2	FIA_UID.2.1
FIA_UID.2.1	FIA_UID.2.1
FIA_UAU.6.1	FIA_UAU.6.1
FIA_UAU.2.1	FIA_UAU.2.1
FPT_ITI.1.1	FPT_ITI.1.1
FPT_ITI.1.2	FPT_ITI.1.2
FPT_ITC.1.1	FPT_ITC.1.1
FPT_ITA.1.1	FPT_ITA.1.1
FDP_DAU.1.1	FDP_DAU.1.1
FDP_DAU.1.2	FDP_DAU.2.2
FDP_DAU.2.1	FDP_DAU.1.1
FDP_DAU.2.2	FDP_DAU.2.2
XCG_CGE.1.1	FXT_XCG.1.1
XCG_CGE.1.2	FXT_XCG.1.2
XCG_CGE.1.3	FXT_XCG.1.3
XCG_CGE.2.1	FXT_XCG.1.4
XCG_CGE.2.2	FXT_XCG.1.6
XCG_CGE.2.3	FXT_XCG.1.6_QC



XCG_CRE.1.1	FXT_XCG.2.3
XCG_CRE.2.1	FXT_XCG.2.4
FCO_POM.1.1	FXT_XGE.1.1
FCS_CKM.1.3	FXT_XKM.1.3
FCS_CKM.3.2	FXT_XKM.3.1
FCS_CKP.3.2	FXT_XKM.6.5
FCS_CKP.1.2	FXT_XKM.6.7
FCS_CKP.1.3	FXT_XKM.7.1
XR_CAP.1.1	FXT_XR.1.1, FXT_XR.1.6
XR_CAP.2.1	FXT_XR.1.3
XR_CAP.1.2	FXT_XR.1.4
FDP_ITT.1.1	FXT_XR.2.1
XRM_CSC.1.2	FXT_XRM.1.2
XRM_CSC.1.1	FXT_XRM.1.3
XRM_CSC.1.3	FXT_XRM.1.4
XRM_CSC.2.1	FXT_XRM.1.6
XRM_CSR.1.1	FXT_XRM.2.2
XRS_RSD.1.1	FXT_XRS.1.1
XRS_RSD.2.1	FXT_XRS.1.2
XRS_SRR.1.1	FXT_XRS.2.1
XRS_SRR.1.2	FXT_XRS.2.4
XTS_REG.2.1	FXT_XTS.3.1
XTS_REG.2.3	FXT_XTS.3.3
XTS_REG.2.4	FXT_XTS.4.5
XTS_REG.3.1	FXT_XTS.4.6
XSP_SDP.1.1	FXT_XSP.2.1
XSP_ACD.1.1	FXT_XSP.3.2
FDP_ACC.1.1	FIA_UID.2.1, FIA_UAU.2.1, FIA_UAU.6.1

Tabla 6.1. Tabla de asociación entre requisitos funcionales y funciones de seguridad

Medidas de Aseguramiento

Los requisitos de seguridad de aseguramiento impuestos al TOE se satisfacen mediante la Metodología de Desarrollo de Safelayer, la cual ha obtenido el certificado ISO 9001:2000.

Esta Metodología consta de los siguientes documentos:

- Documentos de la compañía que aplican al Departamento de Desarrollo del Software:
    - QM "Safelayer Quality Manual", Code 28348ACB

      En este documento se encuentra la definición del Sistema de Gestión de Calidad de la Compañía.
    - DMP "Document Management Plan", Code 9D495947

      Este documento establece las reglas de control de información y los procedimientos para toda la documentación gestionada por la Compañía.
- Proceso de desarrollo principal
    - DM "Development Methods", Code A2A7DE72

      Este documento define el ciclo de desarrollo desde un punto de vista técnico.
    - SSL "Software Security Lifecycle", Code 51D94682

      Se dan consideraciones adicionales a las medidas de seguridad aplicadas a la implementación del software, y este documento complementa el proceso de desarrollo básico para estos casos.
- Disciplinas generales que soportan el proceso
    - QP "Quality Plan", Code D03B789F

      Auditorías, revisiones y procesos y medidas para asegurar que nuestro proceso de desarrollo del software es excelente y está mejorando continuamente.
    - SM "Software Management", Code 3857D336

      En este documento se describe la organización de la Gestión de Desarrollo, las actividades y las técnicas.
    - CM "Configuration Management", Code 411A0E26

      En este documento se describe el control de versines, códigos de identificación del software, procedimientos de distribución y bifurcaciones del software, y toda la historia de desarrollo.
    - SEM "Security Manual", Code 987EEACF

      Productos seguros pueden obtenerse únicamente en un entorno de desarrollo seguro, y este documento regula los procedimientos de seguridad de desarrollo.



- Procedimientos detallados que aplican a áreas y actividades específicas
  - CA "Corrective Action Procedure", Code 07097C4E

    Este documento detalla el procedimiento y la documentación para gestionar acciones correctivas que no pueden ser gestionadas mediante el sistema Bugzilla. Esto incluye típicamente aquellas acciones no asociadas al producto o al código fuente.

  - PA "Preventive Action Procedure", Code 4BAB6D93

    Este documento detalla el procedimiento y la documentación para gestionar acciones preventivas.

  - PM "Safelayer C++ Programming Stylebook", Code 065F6894

    Reglas de programación y convenciones para el lenguaje C++.

  - SP " Safelayer Scryptor Programming Stylebook", Code 88F5BCCD

    Reglas de programación y convenciones para el lenguaje Scryptor.

  - GOC "Guía para la Organización de Código Fuente en Safelayer ", Code 78FC96FB

    Reglas y recomendaciones para organizar los ficheros de código y binarios en un proyecto.

    Etiquetas y reglas de compilación.

  - GTU "Guía para la Implementación de Tests Unitarios en C++", Code B8238977

    Una guía para estructurar y desarrollar pruebas en C++ usando la metodología de test de Safelayer.

  - TS "Creación y Utilización de Tests Unitarios de Scryptor", Code FF4C8949

    Las mismas reglas y convenciones pero aplicadas a los tests de Scryptor.

  - CCS "Control de Configuración en Safelayer con WinCvs", Code 0347E6C0

    Cómo ser un buen usuario del cvs.

  - BUG "Safelayer Bugzilla Usage Guidelines", Code A790CDA4

    Describe el uso de la base de datos de Propuestas de Cambios de Diseño y el sistema de soporte.

  - DSUG "Manual de Usuario del Servidor de Documentación de Safelayer", Code 5C4AC6D9

    Guía de usuario del sistema de gestión de documentos que da sentido a estas referencias.

  - PDP "Product Secure Delivery Procedures", Code 2DB0CC43

    Detalla los procedimientos de entrega con los apropiados niveles de seguridad.



- GL "Gestión de Licencias", Code 300AC51A

  Procedimientos para generar los "Custs" y el proceso y firma de distribuciones.

El cumplimiento de los requisitos de aseguramiento seleccionados se soporta mediante documentación del TOE específica, tal y como se identifica en la siguiente tabla:



Clase de Aseguramiento	Requisito de Aseguramiento	Título del Documento (ID del Documento)
Gestión de Configuración	ACM_CAP.2	Configuration Management (411A0E26) Safelayer Bugzilla Usage Guidelines (A790CDA4)
Entrega y Operación	ADO_DEL.1	Product Secure Delivery Procedures (2DB0CC43)
	ADO_IGS.1	Installation and Uninstallation Tool Manual (B84D4B36) KeyOne 2.1 - Script Signing (DB4586F8) Firma de scripts (7F437D21) KeyOne CA 2.1 - Installation (A2362E54) Manual de instalación KeyOne CA (D1A584E2) KeyOne CA 2.1 - Start-up and maintenance (9A08B9AA) Manual de puesta en marcha y mantenimiento de KeyOne CA (E04DC2FD) KeyOne CA online server 2.1 – Installation (74CBAD1C) Manual de instalación de KeyOne CA Online (B37DFA60) KeyOne CertStatus Server 2.1 - Start-up Manual (F8690A83) Manual de puesta en marcha de KeyOne CertStatus Server (FFD5B9EE) KeyOne LRA 2.1 - Installation and Start-Up (8B9C0115) Manual de instalación y puesta en marcha de KeyOne LRA (4566017C) KeyOne VA 2.1 – Manual (D967013A) Manual de KeyOne VA (28446A95) KeyOne 2.1 - PSS Manager (BC34FCB0) PSS Manager (01D88E2B)

Clase de Aseguramiento	Requisito de Aseguramiento	Título del Documento (ID del Documento)
Entrega y Operación	ADO_IGS.1	KeyOne TSA Server 2.1 – Manual (234BC855) Manual de KeyOne TSA (483BF688) Configuration Guide – CC EAL2 Certification (0F92B8A5) KeyOne 2.1 – KeyOne PSS Generation and Management Tools (DEF348B7) Herramientas de generación y gestión del PSS de KeyOne (7C10F861) KeyOne 2.1 – Starting Up KeyOne Applications with HSM (C9FD2693) Puesta en marcha de aplicaciones KeyOne con HSM (B0E8748E)
Desarrollo	ADV_FSP.1	KeyOne 2.1 Product Specification (4C988209)
	ADV_RCR.1	KeyOne 2.1 Product Specification (4C988209) KeyOne 2.1 High Level Design (BFC2D727)
	ADV_HLD.1	KeyOne 2.1 High Level Design (BFC2D727)



Clase de Aseguramiento	Requisito de Aseguramiento	Título del Documento (ID del Documento)
Documentos de Guía	AGD_ADM.1	KeyOne CA 2.1 - Start-up and maintenance (9A08B9AA) Manual de puesta en marcha y mantenimiento de KeyOne CA (E04DC2FD) KeyOne LRA 2.1 - Programmer's Manual (788E23F1) Manual de programador de KeyOne LRA (2387732D) KeyOne 2.1 - Online Management for KeyOne Servers (D764F939) Administración online de servidores KeyOne (CFBB107C) KeyOne VA 2.1 – Manual (D967013A) Manual de KeyOne VA (28446A95) KeyOne TSA Server 2.1 – Manual (234BC855) Manual de KeyOne TSA (483BF688) KeyOne LRA 2.1 - Installation and Start-up (8B9C0115) Manual de instalación y puesta en marcha de KeyOne LRA (4566017C)
	AGD_USR.1	KeyOne CA 2.1 - User Manual (02F6A136) Manual de usuario de KeyOne CA (6CED5A67) KeyOne LRA 2.1 Programmer's Manual (788E23F1) Manual de programador de KeyOne LRA (2387732D) KeyOne VA 2.1 – Manual (D967013A) Manual de KeyOne VA (28446A95) KeyOne TSA Server 2.1 – Manual (234BC855) Manual de KeyOne TSA (483BF688)



Clase de Aseguramiento	Requisito de Aseguramiento	Título del Documento (ID del Documento)
Pruebas	ATE_COV.1	Quality Assurance-Test Description (C4484186) Quality Assurance-Test Result (47C18C40)
	ATE_FUN.1	Quality Assurance-Test Description (C4484186) Quality Assurance-Test Result (47C18C40) Escenario de Pruebas – Departamento de Calidad (436EFD02)
	ATE_IND.2	Quality Assurance-Test Description (C4484186) Quality Assurance-Test Result (47C18C40) Escenario de Pruebas – Departamento de Calidad (436EFD02)
Análisis de Vulnerabilidad	AVA_SOF.1	KeyOne 2.1 Vulnerability Analysis (08990450)
	AVA_VLA.1	



Cumplimiento de requisitos

En esta sección se justifica cómo algunos requisitos se satisfacen. La sección incluye justificación para los requisitos funcionales y requisitos de aseguramiento.

Cumplimiento de requisitos funcionales

Esta sección incluye una justificación de cómo se cumplen algunos requisitos funcionales. Los requisitos que se satisfacen mediante una única función de seguridad no se incluyen en esta sección, porque el cubrimiento del requisito por la función se describe claramente en la sección Funciones de seguridad del TOE (la sección Tabla de asociación entre requisitos funcionales y funciones de seguridad describe una asociación entre funciones de seguridad y requisitos funcionales).

Requisito XR_CAP.1.1

El requisito XR_CAP.1.1 requiere que las Peticiones de Certificación deben protegerse antes de ser enviadas desde el Servicio de Registro al Servicio de Certificación, de tal manera que se aseguren los servicios de confidencialidad, autenticación e integridad, usando las claves de Control e Infraestructura. Este requisito puede ser asegurado mediante las funciones FXT_XR.1.1 y FXT_XR.1.6.

Cuando la petición de certificación se genera, entonces ésta se inserta en un lote de certificación KeyOne. El operador de Autoridad de Registro firma este lote en el componente KeyOne LRA usando la clave de control de KeyOne LRA. Esta firma se inserta en el lote (campo `signature`), y ésta es validad por el Sistema de Certificación (componente KeyOne CA). El Sistema de Certificación también valida que el certificado asociado a la firma del lote ha sido instalado en el componente KeyOne CA como un certificado de una Autoridad de Registro reconocida.

La firma del lote se provee mediante la función FXT_XR.1.6 y ésta garantiza los servicios de integridad y autenticación aplicados a las Peticiones de Certificación contenidas en el lote KeyOne.

Después de hacer uso de la función FXT_XR.1.6, se invoca la funcionalidad ofrecida por la función FXT_XR.1.1. Esta función envía el lote firmado KeyOne mediante el protocolo SSL/TLS. El proceso de comunicación entre KeyOne LRA y KeyOne CA se establece usando SSL/TLS con autenticación de cliente. El protocolo SSL/TLS establecido por la función FXT_XR.1.1 asegura la confidencialidad de los datos implicados en la comunicación (lote de certificación contiene peticiones de certificación).

Requisito FDP_ACC.1.1

El requisito FDP_ACC.1.1 fuerza el control de acceso basado en mecanismos de identificación y autenticación. Estos controles aseguran que los recursos del sistema y las operaciones ofrecidas por la aplicación son accedidas únicamente por personal autorizado.



Las funciones de seguridad que aseguran este requisito son las siguientes: FIA_UID.2.1, FIA_UAU.2.1 y FIA_UAU.6.1.

Los controles asegurados por el requisito FDP_ACC.1.1, son establecidos inicialmente por la función de seguridad FIA_UID.2.1, que implementa los mecanismos de identificacion necesarios para acceder a la aplicación. Cuando el usuario ha sido identificado, entonces se ejecuta la función de segurida FIA_UAU.2.1; esta función implementa el mecanismo de autenticación implantado en el sistema. En en el caso de que sea necesario un mecanismo de re-autenticación, entonces se invoca la función de seguridad FIA_UAU.6.1.

Funciones de Seguridad que utilizan algoritmos criptográficos

Las siguientes funciones de seguridad descritas en "*KeyOne 2.1 – Functional Specification*, código interno: 4C988209" hacen uso de mecanismos criptográficos.

Función de Seguridad
FAU_GEN.1.1
FAU_GEN.1.2
FAU_STG.1.1
FAU_STG.1.2_1
FAU_STG.1.2_2
FCS_CKM.1.1_1
FCS_CKM.2.1
FCS_CKM.3.1
FCS_COP.1.1_1
FXT_XKM.1.3
FXT_XKM.1.7
FXT_XKM.3.1
FXT_XKM.6.5
FIA_UID.1.1
FIA_UID.2.1
FIA_UAU.2.1
FIA_UID.6.1



FPT_ITI.1.1
FPT_ITI.1.2
FPT_ITC.1.1
FDP_DAU.1.1
FDP_DAU.2.2
FXT_XCG.1.1
FXT_XCG.1.3
FXT_XCG.1.6
FXT_XCG.1.6_QC
FXT_XCG.2.3
FXT_XCG.2.4
FXT_XGE.1.1
FXT_XR.1.1
FXT_XR.1.4
FXT_XR.1.6
FXT_XR.2.1
FXT_XRM.1.2
FXT_XRM.1.4
FXT_XRS.1.2
FXT_XRS.2.1

CAPÍTULO 7

Reivindicaciones

En estos Objetivos de Seguridad no se reivindica ningún perfil de protección.

Sin embargo, es relevante notar que los requisitos de seguridad que se establecen en este documento son equivalentes a los que se especifican en [CEN01c], aunque no se abarcan len su totalidad ni se puede proclamar la conformidad con los ellos.

Razonamiento

Security Objectives Rationale

As the security objectives are stated either to counter identified threats and to cover the policies, the justification will be explained in two distinct ways, separating TOE security objectives from environmental security objectives.

It is important to notice that a complete coverage of all Organizational Security Policies are enforced by the TOE and the environment security objectives, considering the secure usage assumptions made in chapter three.

Security Objectives Coverage

All the threats identified are able to damage whatever of the security assurances of TOE assets, as integrity, confidentiality and availability, so they are countered by at least one objective for each security assurance.

Objectives - Threats – Policies- Assumptions Mapping Table

		O1	O2	O3	O4	O5	O6	O7	O8	O9
Threats	***T1***	X	X	X		X		X	X	X
	T2				X	X	X			
	T3	X	X	X		X	X	X	X	X
Policies	***P_SO1.1***	X			X	X	X			



	P_SO3.1				X		X			
	P_IA1.1		X							
	P_IA1.2		X							
	P_KM1.1								X	
	P_KM1.3						X			
	P_KM1.4						X			X
	P_KM1.7						X			
	P_KM2.1						X			X
	P_KM2.2						X	X		
	P_KM2.3	X					X			
	P_KM2.4	X	X		X					
	P_KM2.5	X					X	X		
	P_KM2.6	X	X				X			
	P_KM3.1		X				X		X	
	P_KM3.4				X					
	P_KM3.5		X				X		X	
	P_KM3.6				X					
	P_KM4.1				X		X			
	P_KM4.2						X			
	P_KM5.1						X			
	P_KM5.2			X			X			
	P_KM6.1			X			X			
	P_KM6.3			X						X
	P_KM6.4			X						X
	P_KM6.5		X						X	
	P_KM6.6		X				X		X	
	P_KM6.7			X	X		X			
	P_KM7.1			X	X		X			
	P_AA2.2	X								



	P_AA3.1		X			X		X		
	P_AA4.1		X			X	X			
	P_AA4.2		X			X				
	P_AA5.2							X		
	P_AA7.1	X					X			
	P_AA8.1						X			
	P_AR1.1		X			X		X		
	P_AR1.2		X			X			X	
	P_AR1.3				X		X	X		
	P_AR1.4			X						
	P_AR2.1		X		X	X				
	P_AR3.1	X						X		
	P_BK1.1					X				
	P_BK1.2					X				
	P_BK1.3						X		X	
	P_BK2.1	X						X		
	P_BK2.2			X			X			
	P_BK3.1					X	X			
	P_BK3.2						X		X	
	P_GE.1	X		X			X	X		
	P_R1.1			X						
	P_R1.2		X							
	P_R.1.3				X	X				
	P_R.1.4		X							
	P_R.1.6	X	X							
	P_R.2.1			X						
	P_R.3.1		X			X				
	P_CG1.1	X	X	X						
	P_CG1.2				X		X			



	P_CG1.3				X					
	P_CG1.4				X					
	P_CG1.6				X					
	P_CG1.6-QC				X					
	P_CG2.3				X					
	P_CG2.4	X	X	X						
	P_RM1.1				X	X				
	P_RM1.2		X		X					
	P_RM1.3				X					
	P_RM1.4				X					
	P_RM1.6				X	X				
	P_RM2.2				X	X				
	P_RM3.1		X						X	
	P_RS1.1		X		X					
	P_RS1.2	X	X							
	P_RS2.1	X	X							
	P_RS2.2				X					
	P_RS2.4		X		X	X				
	P_RS3.1		X							
	P_TS1.1								X	
	P_TS1.2						X			
	P_TS2.1				X					
	P_TS2.2						X			
	P_TS3.1				X	X				
	P_TS3.2						X			
	P_TS3.3				X					
	P_TS4.1						X			X
	P_TS4.5	X						X		

	P_TS4.6				X					
	P_TS6.1		X		X	X				
	P_SP2.1		X						X	
	P_SP3.1						X	X	X	
	P_SP3.2				X		X			X
Assumptions	***H1***						X			X
	H2					X	X	X	X	X
	H3					X	X			
	H4									X
	H5						X	X		X
	H6						X			
	H7						X			
	H8						X			
	H9					X				
	H10					X		X		X
	H11									X
	H12						X			

Table 8.1

Security Objectives Sufficiency

Demonstration of the sufficiency of Security Objectives for adequately protect critical TOE assets is fully explained in this section.

Threats and Security Objective Sufficiency

T1. Violation of security policies and certificate practice statement.

This threat can cause a lack of integrity in any of the TOE assets identified, which is countered by the **TOE integrity objective (O1)**, protecting TOE systems an products, together with **O7 Databases and Operating systems Integrity**, protecting the integrity of the supporting environment.

Relating disclosure of critical information, **TOE confidentiality objective (O3)** is intended to protect sensitive TOE assets as secret keys against leakage information while **O9 Confidentiality of Security Devices** is avoiding any misuse of process of generating signature-creation data for QC/NQC signing certificates and for



registration officers authentication mechanism as well as management and administration processes of security devices.

O2. Authentication & Accountability and O8 A&A of environment, are intended to provide protection mechanisms to detect and register this type of actions, for further investigations.

With regards to real-time services as revocation, validation and time stamping services, this threat can cause unavailability or delays in service delivery. These attacks are countered by **O5 Availability**.

T2. Code exploitation.

Exploitation of TOE vulnerabilities or security flaws, resulting from engineering software processes that have not been identified on time. This threat is primary countered at software development level by **O4 Assurance** and at delivery and operation level by **O5 Availability** and **O6 Trusted environment**.

T3. External Attacks.

This type of attacks usually can result in unauthorized interception and modification threats which can damage TOE security assurances in different ways:

Lack of integrity of data exchanged between TOE components and user interfaces (A5) that is countered by **O1 – TOE integrity** and **O7 – Databases and Operating Systems Integrity**.

If potential intruders or impersonation attacks trying to gain access in a malicious way **O2 – Authentication & Accountability**, is intended to maintain appropriate access control, preventing unauthorized user access to TOE information systems. This is also applicable to the TOE environment, which is ensured with **O6 – Trusted Environment and O8 A&A of environment**.

Regarding to loss of confidentiality, any sensitive information leakage is countered by **O3 – Confidentiality and O9- Confidentiality of Security Devices**.

Preventing any interruption of services, and/or unavailability of TOE assets A6, A7, A8, A9 and A10, is countered by **O5 – Availability**.

Organizational Security Policies and Security Objectives Sufficiency

All the following policy requirements which are designed to preserve integrity of whatever TOE data, process and operation are generally enforced by **O1 – TOE integrity and O7 –Databases and Operating systems Integrity,** as described here**:**

P.SO to upheld the integrity and accuracy of the TOE systems and information.

P.SO1.1, protect the integrity of TOE software and configuration system

P.KM Key Management Organizational Policies which state requirements for generation, distribution, usage, storage, backup & recovery and archival of keys, are the main mechanism for providing integrity of TOE assets.

P.KM.2.3, integrity of key distribution method,

P.KM.2.2, prevent manipulation of public keys not yet certified

P.XM.2.4, integrity of public keys,

P.XM.2.5, integrity of self-signed certificate,

P.KM.2.6. provide fingerprint mechanisms to ensure the integrity of some kind of digital signatures

P.AA Authentication & Accounting, preserving integrity of accounting and auditing information:

P.AA.2.2 Prevent audit rewriting,

P.AA.3.1 Requirement of audit registration,

P.AA.5.2 Preventing modifications of the audit records,

P.AA.7.1 guarantee audit data integrity,

P.AR To ensure the integrity of archived data

P.AR.1.1, ensure generation of an integrity archiving,

P.AR.1.3 , including accurate timing data,

P.AR.3.1, protect from modification,

P.BK to ensure the integrity of backup information

P.BK.2.1. Backups protected from modification

P.GE to safeguard integrity of messages exchanged through internal and external interfaces

P.GE.1. protect integrity of messages exchanged,

P.RS, integrity of data provided by Registration Service

P.R.1.6, integrity of certificate requests,

P.CG, integrity of data provided by Certificate Generation Service

P.CG1.1, integrity of certificate request messages,

P.CG2.4, integrity of re-certificate request messages,

P.CRSS, integrity of data provided by Certificate Revocation Status Service

P.RS.1.2, integrity of revocation management entity,

P.RS.2.1, integrity of entity issuing revocation status messages,

P.TSS, integrity of data provided by TSA

P.TSS.4.5, ensuring consistency in data generated by TSA

P.SDPS, ensures the integrity of critical information and its supporting devices

P.SP.3.1 generating initial activation data securelyRegarding policy requirements which are designed in someway to preserve authentication and accountability are enforced by **O2 – TOE Authentication & Accounting and O8 – A&A of environment**:



P.IA To ensure secure access and use of the TOE systems and information.

P.IA1.1, ensure secure identification and authentication mechanisms,

P.IA1.2, ensure re-authentication mechanisms after log-out,

P.KM Key Management Organizational Policies which state requirements for generation, distribution, usage, storage, backup & recovery and archival of keys, are the main mechanism for providing integrity

P.XM.2.4, authenticity of publicic keys,

P.KM.1.1, provide access control mechanism and confidentiality for the certificates signing keys.

P.KM.2.6. provide fingerprint mechanism for authenticity of some digital signatures,

P.KM.3.1, Access control mechanisms for all SCD's

P.KM.3.5, Authorized key usage only during operational life,

P.KM.6.5, only authorized personnel can backup, restore and storage of secret keys,

P.KM.6.6, only dual control access is permitted for doing backup, restore and storage of secret keys,

P.AA Authentication & Accounting, preserving integrity and availability of accounting records

P.AA.3.1 requirement of audit registration,

P.AA.4.1 Ensure selectable audit information,

P.AA.4.2, and suitable to interpret,

P.AR To ensure the secure access of archived information

P.AR.1.1, capability of generating an archive for subsequent processing in providing necessary legal evidence

P.AR.1.2 requirement of minimum archival information

P.AR.2.1 Ensure selectable archiving information

P.BK to ensure a secure access to backup information

P.BK.1.3 a user with sufficient privileges is able to invoke backup function,

P.BK.3.2 a user with sufficient privileges is able to invoke recovery function,

P.RS, authentication and accounting of registration service

P.R.1.2 Secure authentication of a holder private Key

P.R.1.4 Secure authentication of certificate application,

P.R.1.6 Certificate requests must be signed for authentication purposes,



P.R.3.1Generate accounting information from registration service,

P.CGS, ensures the data origin authenticity of this service

P.CG.1.1 ensure data origin authenticity of certificate request message,

P.CG.2.4 Secure authentication of re-certificate application

P.CRMS, authentication and accounting of revocation management service

P_RM.1.2, authentication and validation of requests

P_RM.3.1, Revocation Management Audit

P.CRSS, authentication and accounting of revocation status service

P_RS1.1, authenticate trusted revocation service,

P.RS.1.2, authenticity of revocation management entity,

P.RS.2.1, authenticity of entity issuing revocation status messages,

P.RS.2.4, response message must contain the time

P.RS.3.1, generate accounting information from this service

P.TSS, authentication and accounting of TSA functions

P.TS.1.1, control the origin of time-stamping requests

P.TS.6.1, ensures archiving of TST's

P.SDPS, ensures the authentication and accounting of critical information and its supporting devices

P.SP.2.1 The SCDev must be distributed to the authenticated subject

P.SP.3.1 generating initial activation data securely

Regarding policy requirements which are designed in someway to preserve confidentiality of critical assets are enforced by **O3 – TOE Confidentiality and O9 – Confidentiality of Security Devices**

P.KM Key Management Organizational Policies which state requirements for generation, distribution, usage, storage, backup & recovery and archival of keys, are the main mechanism for providing confidentiality

P.KM.1.4. Infrastructure and control keys must be generated and maintained in a HCD,

P.KM.2.1. Secret keys must not be distributed in plain text

P.KM.5.2. systems use to generate, use or store secret keys must be destroyed,

P.KM.6.1, Secure store of private keys,

P.KM.6.3, some private keys must be stored in a Hardware Cryptographic Device,

P.KM.6.4. sensitive key material must be protected from disclosure



P.KM.6.7. no functions exist for backup Subject signature keys,

P.KM.7.1. no functions exist for archiving Subject signature keys

P.SDPS, ensures the authentication and accounting of critical information and its supporting devices

P.SP.3.2 ensuring the non misuse of the SCDev at any time.

P.BK to ensure a secure access to backup information

P.BK2.2 protect sensitive information from disclosure

P.AR To ensure the secure access of archived data

P.AR.1.4 ensure protection of critical security parameters

P.GE to safeguard confidentiality of messages exchanged through internal and external interfaces

P.GE.1. protect confidentiality of messages exchanged,

P.RS, confidentiliaty of registration service

P.R.1.1 protect subject sensitive information in certificate application process,

P.R.2.1 protect the privacy and confidentiality of Subject information.

P.CGS, ensures the privacy and confidentiality of this service

P.CG.1.1 ensure privacy and confidentiality of certificate request message, when necessary,

P.CG.2.4 privacy and confidentiality of re-certificate application,

Regarding policy requirements which are designed in someway to preserve regulations and standards compliance are enforced by **O4 – TOE Assurance and O6 – Trusted Operating environment**:

P.SO to upheld the assurance of TOE functionality

P.SO1.1correctly and securely operation

P.SO3.1, ensure time synchronization between components

P.TSS, authentication and accounting of TSA functions

P.TS.2.2, obtaining acceptable and valid times

P.KM Key Management Organizational Policies which state requirements for generation, distribution, usage, storage, backup & recovery and archival of keys.

P_KM.3.1, Access control mechanism for all SCD's,

P_KM.3.5, Authorized key usage only during operational life,

P_KM.4.2, Changeover carried out securely,

P_KM.5.1, Secure key destruction,

P_KM.5.2, Systems use to generate, use or store secret keys must be destroyed,

P_KM.6.1 Secure store of private keys,

P_KM.1.3 Dual person control is required to access secure cryptographic modules,

P.KM.1.4. Infrastructure and control keys must be generated and maintained in a HCD,

P.KM.1.7. Key generation shall meet [ALGO],

P.KM.2.1. Secret keys must not be distributed in plain text

P.KM.2.2, prevent manipulation of public keys not yet certified

P.XM.2.4, made public keys available to relying parties,

P.XM.2.5, specific properties relating self-signed certificate must be satisfied,

P.KM.2.6. the fingerprint must fulfilled hashing algorithms specified in [ALGO]

P_KM.3.4, ensure certificate policy requirement,

P.KM.3.6 Key validation before use

P_KM.4.1, change infrastructure and control keys on a regular basis,

P.KM.6.6, only dual control access is permitted for doing backup, restore and storage of secret keys,

P.KM.6.7. no functions exist for backup Subject signature keys,

P.KM.7.1. . no functions exist for archiving Subject signature keys

P.AA assurance of accounting records

P.AA.4.1 Ensure selectable audit information,

P.AA.7.1 guarantee audit data integrity,

P.AA.8.1 A trusted time source should be used to mark the time of audit event

P.AR To fulfil requirements for archiving

P.AR.1.3 , including accurate timing data

P.AR.2.1 , with capability for searching

P.BK to ensure a secure access to backup information

P.BK.1.3 a user with sufficient privileges is able to invoke backup function,

P.BK.2.2. critical security parameters must be protected with encryption fulfilling [ALGO],

P.BK3.1, include a recovery function

P. BK3,2, only privilege roles can invoke recovery function



P.GE assurance of messages exchanged through internal and external interfaces

P.GE.1. contain a message time of the creation,

P.RS, assurance of registration service

P.R.1.3 information collected from subscriber

P.CGS, assurance of this service

P.CG.1.2 certificate request must conform with the applicable policy

P.CG.1.3 validation of Proof of Posesion must be validated before processing

P.CG.1.4 restriction on QC signing key usage

P.CG.1.6 (y QC) certificate must conform with specific properties

P.CG.2.3 Procedures to re-certificate

P.CRMS, assurance of revocation management service

P_RM.1.1, revocation management process has timely restrictions to fulfilled

P_RM.1.2, authentication and validation of requests

P_RM.1.3, a revoked certificate can not be reinstated

P_RM.1.4, At least dual control is required to revoke QC/NQC signing keys

P_RM.1.6, certificate status database must be updated immediately

P_RM.2.2, status repository must be updated on a regular basis

P.CRSS, assurance the conformance with Certificate Policies and CPS

P.RS.1.1 input messages to this service must be from trusted RMS

P.RS.2.2, the signing of status responses must fulfilled [ALGO]

P.RS.2.4 the responses messages must contained the time at which issuer signed the response

P.TSS, assurance the conformance with Certificate Policies and CPS

P.TS.1.2, the requests for Time Stamping uses a hash algorithm approved by [ALGO]

P.TS.2.1 the TSA must be synchronized to UTC with 1 second of tolerance

P.TS.3.1, the serial number of the TST must be unique for each TST issued by a given TSA,

P.TS.3.2 information about the accuracy of the time source must be included in the TST if exceeds that required by TSA policy,

P.TS.3.3, policy for the creation of TST,

P.TS.4.1, TSA signing keys must be generated and stored in a secure cryptographic module,

P.TSS.4.6 using cryptographic algorithms to generate TST

P.TS.6.1, all the TST's must be archived

P.SDPS, ensures assurance of this service

P.SP.3.1 generating initial activation data securely

P.SP.3.2 The CSP's personnel can not misused the SCDev at any time, by procedures or other mechanisms

Regarding availability and timeliness policies, they are enforced mainly by the environment **O5 .TOE Availability:**

P.SO to upheld the assurance of TOE functionality

P.SO1.1 prevent system failure

P.AA availability of accounting records

P.XAA.3.1 audit records must contain specific parameters

P.XAA.4.1 capability to search for events

P.XAA.4.2 presented in a manner suitable for interpretation

P.AR To fulfil requirements for archiving

P.AR.1.1, provide an archive on media appropriate for storage and access when required

P.AR.1.2 , Content archiving requirements policy

P.AR.2.1 Ensure selectable archiving information

P.BK to ensure a secure access to backup information

P.BK.1.1 , include a backup function

P.BK.1.2 sufficient to recreate the state

P.BK.3.1, include a recovery function

P.RS, availability of registration service

P.R.1.3 information collected from subscriber

P.R.3.1Generate accounting information from registration service,

P.CRMS, revocation management timeliness

P.RM.1.1, provide revocation service in a timely manner

P_RM.1.6, certificate status database must be updated immediately

P_RM.2.2, status repository must be updated on a regular basis

P.CRSS, availability of revocation status service

P.RS.2.4, response message must contain the time



P.TSS, authentication and accounting of TSA functions

P.TS.3.1, the property of TST uniqueness must be preserved even after an interruption

P.TS.6.1, all the TST's must be archived

Security Requirements Rationale

Up to this point, Security Objectives have been identified, to cover both the general threats against the TOE and Organizational Policy Statements. These Security Objectives have also been assigned both to the TOE and to the Environment, by application of the active Assumptions.

For those Security Objectives assigned to the TOE, Security Requirements already identified in Sec. 5 are selected and a justification of those implemented by the TOE is also provided to demonstrate coverage and sufficiency.

Security requirements Coverage

The following mapping table shows how TOE security requirements cover all the TOE security objectives:

TOE Security Requirement / TOE Security Objective	*O1*	*O2*	*O3*	*O4*
FAU_GEN.1.1		X		X
FAU_GEN.1.2		X		X
FAU_GEN.2.1		X		
FAU_SAR.1.1		X		
FAU_SAR.1.2		X		
FAU_SAR.3.1		X		
FAU_STG.1.1	X	X		
FAU_STG.1.2_1	X	X		
FAU_STG.1.2_2	X	X		
FCS_CKM.1.1_1			X	
FCS_CKM.1.1_2	X	X		
FCS_CKM.2.1	X	X	X	
FCS_CKM.3.1		X		X
FCS_COP.1.1_1			X	X
FCS_COP.1.1_2	X	X		X
FCS_COP.1.1_3			X	X

FCS_COP.1.1_4			X	X
FCS_COP.1.1_5		X		X
FDP_ACC.1.1		X		
FIA_UID.1.1		X		
FIA_UID.1.2		X		
FIA_UID.2.1		X		
FIA_UAU.6.1		X		X
FIA_UAU.2.1		X		X
FPT_ITI.1.1	X			
FPT_ITI.1.2	X			
FPT_ITC.1.1			X	
FPT_ITA.1.1	X			X
FDP_DAU.1.1		X		
FDP_DAU.1.2		X		X
FDP_DAU.2.1		X		X
FDP_DAU.2.2		X		X
XCG_CGE.1.1	X	X	X	
XCG_CGE.1.2				X
XCG_CGE.1.3				X
XCG_CGE.2.1				X
XCG_CGE.2.2				X
XCG_CGE.2.3				X
XCG_CRE.1.1		X		X
XCG_CRE.2.1	X	X	X	
FCO_POM.1.1	X		X	
FCS_CKM.1.3		X		X
FCS_CKM.3.2		X		
FCS_CKP.3.2		X		
FCS_CKP.1.2			X	X
FCS_CKP.1.3			X	X
XR_CAP.1.1	X	X	X	
XR_CAP.2.1				X
XR_CAP.1.2		X		



FDP_ITT.1.1	X		X	
XRM_CSC.1.2		X		X
XRM_CSC.1.1				X
XRM_CSC.1.3		X		X
XRM_CSC.2.1				X
XRM_CSR.1.1				X
XRS_RSD.1.1		X		X
XRS_RSD.2.1	X	X		
XRS_SRR.1.1	X	X		X
XRS_SRR.1.2		X		X
XTS_REG.2.1				X
XTS_REG.2.3				X
XTS_REG.2.4	X			
XTS_REG.3.1				X
XSP_SDP.1.1		X		
XSP_ACD.1.1				X
XSM_OPM.1				X
ACM_CAP.2				X
ADO_DEL.1				X
ADO_IGS.1				X
ADV_FSP.1				X
ADV_HLD.1				X
ADV_RCR.1				X
AGD_ADM.1				X
AGD_USR.1				X
ATE_COV.1				X
ATE_FUN.1				X
ATE_IND.2				X
AVA_SOF.1				X
AVA_VLA.1				X

Table 8.2

The table corresponding to the environment requirements is the following:



TOE Security Requirement / TOE Security Objective	*O5*	*O6*	*O7*	*O8*	*09*
FCS_CKM.1.1_2			X	X	X
FCS_CKM.2.1			X	X	X
FCS_CKM.4.1				X	X
FCS_COP.1.1_6			X	X	X
FCS_COP.1.1_7			X	X	X
FCS_COP.1.1_8			X	X	X
FPT_STM.1.1	X				
FDP_DAU.1.1				X	
FDP_DAU.2.1				X	
FPT_STM.2.1	X				
FCS_CKM.1.2				X	X
FCS_CKM.1.3				X	X
FCS_CKM.3.2				X	X
FCS_CKM.4.2				X	X
FCS_CKM.4.3				X	X
FCS_CKP.1.1		X		X	
FCS_CKP.2.1		X		X	
FCS_CKP.2.2		X		X	X
FCS_CKP.3.1		X			X
FCS_CKP.3.2		X			
FCS_KCH.1.1		X			
FCS_KCH.1.2		X			
XR_SDM.1.1		X			X
XCG_CGE.1.1		X		X	
XCG_CGE.2.2		X			
XCG_CGE.2.3		X			
XCG_CRE.1.1		X			
XCG_CRE.2.1		X			
XRM_CSC.1.3		X		X	
XRS_RSD.1.1		X		X	
XTS_REC.1.1		X		X	



XTS_REC.2.1		X			
XTS_REG.1.1	X				
XTS_REG.1.2	X				
XTS_REG.2.2	X				
XTS_REG.3.2		X			X
XSP_ACD.1.2		X			
XAA_RAR.1.1		X	X		
XAA_GAT.1.1	X				
XBK_BAR.1.1		X			
XBK_BAR.1.2		X		X	
XBK_BAR.2.1		X			
XBK_BAR.2.2		X		X	
XSO_OPM.1.1		X			

Table 8.3

Security Requirements Sufficiency regarding to the TOE

Since cryptographic keys are the main mechanism used by the TOE to provide integrity, confidentiality and authentication functions, key management processes are essential to support the security objectives which address those security properties.

So, in general we will notice cryptographic functions **implemented by the class FCS** are relevant to the three TOE security objectives: **O1-Integrity, O2-Identification & Authentication, and O3 – Confidentiality**. To ensure a complete satisfaction of this security services an appropriate key management is required.

Regarding protection of sensitive information from disclosure or alteration when transmitting, **FPT_ITI.1.1, FPT_ITI.1.2, FPT_ITA.1.1, FPT_ITC.1.1 and FDP_ITT.1.1** implement those requirements.

The allowed cryptographic operations and protocols are provided by **FCS_COP.1.1.** The conjunction of those operations provide the required integrity, confidentiality and authentication mechanisms for the TOE assets.

O1- Integrity. The integrity security objective is mainly satisfied by cryptographic mechanisms of TOE systems and functions, which are implemented by the functional family FCS: **FCS_CKM.1.1_2, FCS_COP.1.1_2** and **FCS_CKM.2.1**. Related to audit records the lack of integrity is also detectable by **FAU_STG1.1, FAU_STG1.2_1** and **FAU_STG1.2_2,** and integrity protection of TSF data is implemented by **FPT_ITI.1.1, FPT_ITI.1.2 and FPT_ITA.1.1.**

The integrity of Certificate Generation Service is implemented by **XCG_CGE1.1 and XCG_CRE.2.1.**

The integrity of messages exchanged is implemented by **FCO_POM.1.1.**

The integrity of Registration Service is implemented by **XR_CAP.1.1** and **FDP_ITT.1.1.**

The integrity of Revocation Status Service is implemented by **XRS_RSD.2.1** and **XRS_SRR.1.1.**

The integrity of Time Stamping Service is implemented by **XTS_REG.2.4**

O2 –Authentication & Accountability.
Regarding to accountability of the certification activity be effective for non-repudiation purposes, the following requirements are required:

- Identification of events to be recorded (**FAU_GEN.1.1 Audit Data Generation**)，
- The information to be generated when such an event has occurred (**FAU_GEN.1.2, FAU_GEN.2.1**)，
- Control the access to this information only to authorized users (**FAU_SAR.1.1**)，
- Provide easy access and searching facilities to this information (**FAU_SAR.1.2, FAU_SAR.3.1**)
- Ensure the protection from deletion and modifications of this audit data (**FAU_STG.1.1, FAU_STG1.2_1, FAU_STG1.2_2**)

In order to support authentication security assurances required by this objective, the following requirements are provided:

- Cryptographic Keys for strong authentication purposes (**FCS_CKM.1.1_2)**
- Cryptographic Key distribution mechanism based on public key certificates implemented by **FCS_CKM.2.1**
- Cryptographic key access implemented by **FCS_CKM.3.1**
- A set of Cryptographic operations which ensure authentication and non-repudiation mechanisms **FCS_COP.1.1_2 and FCS_COP.1.1_5**
- Access control mechanisms are implemented for all secure cryptographic modules and its operations (**FCS_CKM1.3, FCS_CKM.3.2, FCS_CKP.3.2**)
- unambiguous identification of authorised users, determining the authority to interact with the TOE, must be implemented （**FIA_UID.1.1, FIA_UID.1.2 FIA_UID.2.1**）
- required user authentication mechanisms must be implemented (**FIA_UAU.2.1, FIA_UAU.6.1, FDP_DAU.1.1, FDP_DAU.1.2, FDP_DAU.2.1, FDP_DAU.2.2, FDP_ACC.1.1)**

The authentication of Certificate Generation Service is implemented by **XCG_CGE1.1, XCG_CRE.1.1 and XCG_CRE.2.1.**

The authentication of Registration Process is implemented by **XR_CAP.1.1, R_CAP.1.2.**

The authentication of Revocation Management Service is implemented by **XRM_CSC.1.2, XRM_CSC.1.3.**

The authentication of Revocation Status Service is implemented by **XRS_RSD.1.1, XRS_RSD.2.1, XRS_SRR.1.1** and **XRS_SRR.1.2.**

The authentication of Subject device Provision Service is implemented by **XSP_SDP.1.1.**



O3 - Confidentiality Again this security objective is satisfied by cryptographic functions for protecting communications links and data containers: **FCS_CKM1.1_1, FCS_CKM2.1**, **FCS_COP.1.1_1**, **FCS_COP.1.1_3**, **FCS_COP.1.1_4, FCS_CKP.1.2 and FCS_CKP.1.3.**

With regards to subscriber data confidentiality, TOE registration process confidentiality is implemented by **XR_CAP.1.1** and **FDP_ITT.1.1**.

With regard to all TSF data transmitted from the TSF to a remote trusted IT product, the confidentiality security service is implemented by the **FPT_ITC.1.1** requirement.

This security objective also covers confidentiality issues stated for ensure privacy and confidentiality of the certificate request message (**XCG_CGE.1.1, XCG_CRE.2.1**) and exchanged messages through internal and external interfaces (**FCO_POM.1.1**).

The **O4 - Assurance Objective** is covered according to an assurance level where developers or users require a low to moderate level of independently assured security, according to CC EAL2. This assurance is provided by an analysis of the security functions using a functional and interface specification (**ADV_FSP.1**), high level design of the TOE (**ADV_HLD.1**), a demonstrated representation correspondence (**ADV_RCR.1**) and guidance documentation (**AGD_ADM.1, AGD_USR**.**1**), to understand the security behaviour; evidence of developer testing based on the functional specification (**ATE_COV.1, ATE_FUN.**1), selective independent confirmation of the developer test results (**ATE_IND.2**), strength of function analysis (**AVA_SOF.1**), and evidence of a developer search for obvious vulnerabilities (**AVA_VLA.1**). Through configuration management process providing a configuration list for the TOE (**ACM_CAP.2**) and also evidence of secure delivery, installation and generation procedures (**ADO_DEL.1, ADO_IGS.1, ADO_OPM.1**).

Otherwise, in order to safeguard TOE security assurances in the operational environment together with the fulfillment of technical standards and regulations fully accepted and recognized, the following requirements has been implemented:

- Specific events for each CSP service MUST be recorded by **FAU_GEN.1.1** and **FAU_GEN.1.2**.
- All the cryptographic operations MUST be conformant with specified cryptographic algorithm and organizational policy standards as implemented in **FCS_COP.1.1 (FCS_COP.1.1_1, FCS_COP.1.1_2, FCS_COP.1.1_3, FCS_COP.1.1_4, FCS_COP.1.1_5)** and **FCS_CKM.3.1** requirements.
- Conditions for authentication and re-authentication according to organizational policies standard are implemented by **FIA_UAU.6.1** and **FIA_UAU.2.1**
- Guarantees of validity of authentication data MUST be provided for subsequent verification, as implemented by **FDP_DAU.1.2**, **FDP_DAU.2.1** and **FDP_DAU.2.2**
- Data collection of Registration Process MUST satisfy specific requirements for QC according to the EU Directive which are implemented by **XR_CAP.2.1**
- Guarantees and properties related to the issued certificates to be conformant with specific standards are implemented by **XCG_CGE.2.1,**

XCG_CGE.2.2, XCG_CGE.2.3, as well as for appropriate operating security procedures as defined in **XCG_CGE.1.2** and **XCG_CGE.1.3**.

- Security requirements for renewal certificate process are implemented by **XCG_CRE.1.1**
- Requirements for conditions and restrictions of revocation / suspension management service are implemented by **XRM_CSC.1.1, XRM_CSC.1.2, XRM_CSC.1.3, XRM_CSC.2.1, XRM_CSR.1.1**
- Specific conditions for availability of Revocation Status Service MUST be fulfilled and are implemented by **FPT_ITA.1.1.,** as well as for its trusted operation provided by **XRS_RSD.1.1** and trusted communications with relying parties provided by **XRS_SRR.1.1** and **XRS_SRR.1.2**
- Security requirements for certain key generation process is implemented by **FCS_CKM.1.3**
- Restrictions for specific operations to Subject signature keys are implemented by **FCS_CKP.1.2** and **FCS_CKP.1.3**
- Time Stamping service MUST issue TST conformant with specific policies implemented by **XTS_REG2.1** and **XTS_REG.2.3** and implement mechanisms to ensure the security of Time-Stamp responses (**XTS_REG3.1**)
- Security requirements for the generation of activation data is implemented by **XSP_ACD.1.1**

Security Requirements Sufficiency regarding to the Environment

Since cryptographic keys are the main mechanism used by the environment to provide authentication of environment computing resources and confidentiality of security devices, key management processes are essential to support the security objectives which address those security properties.

So, in general we will notice cryptographic functions **implemented by the class FCS** are relevant to the two environment security objectives: **O8-Authentication & Accountability of environment computing resources and O9 – Confidentiality of Security Devices**. To ensure a complete satisfaction of this security services an appropriate key management is required.

O5- Availability of critical assets A6, A7, A8, A9 and A10. This objective is satisfied by the **XAA_GAT.1.1, FPT_STM.1.1, FPT_STM.2.1, XTS_REG.1.1, XTS_REG.1.2** and **XTS_REG.2.2** requirements. This requirement introduces guarantees regarding to the time used by the system.

O6 –Trusted operational environment
Regarding to procedures and controls, the following requirements are required over the keys managed by the environment:

- Controls in order to prevent interception in public keys that have not been certified (**FCS_CKP.1.1**).



- Controls in order to not distribute in plain text and never store in an unprotected state the private and secret keys (**FCS_CKP.2.1, FCS_CKP.2.2**).
- Controls in order to access the private/secrets keys, Infrastructure keys, control keys and NQC/QC signing keys (**FCS_CKP.3.2**).
- Controls in order to used a secure storage mechanism for the private/secrets keys, Infrastructure keys and control keys (**FCS_CKP.3.1**), and for the TSA Signing key and TSA Control Keys (**XTS_REG.3.2**).
- Controls in order to securely renew the Infrastructure and control keys (**FCS_KCH.1.1** and **FCS_KCH.1.2**), QC/NQC signing keys (**XCG_CRE.1.1**) and Subscriber keys (**XCG_CRE.2.1**)

Procedures and controls that assure the privacy and confidentiality of the Subject Information are implemented by **XR_SDM.1.1**.
Procedures and controls that assure security services applied to the request message are implemented by **XCG_CGE.1.1** and **XTS_REC.1.1**.
Procedures and controls that assure that the generated certificates accomplish with an established and secure profile are implemented by **XCG_CGE.2.2** and **XCG_CGE.2.3**.
Procedures and controls that establish secure revocation conditions for the QC/NQC signing keys are implemented by **XRM_CSC.1.3**.
Procedures and controls that establish conditions for periodical messages provided by the Revocation Status Service are implemented by **XRS_RSD.1.1**.

Procedures and controls in order to minimize the risk of systems are assured through the **XSO_OPM.1.1** requirement.

Procedures and controls over the time stamp request are implemented by the **XTS_REC.1.1** requirement.
Procedures and controls in order to prevent modification of the audit database are implemented by the **XAA_RAR.1.1** requirement.
Procedures and controls in order to active data creation in the SCDev are implemented by the **XSP_ACD.1.2 r**equirement.
Procedures and controls in order to backup and recovery the system are implemented by the following requirements: **XBK_BAR.1.1, XBK_BAR.1.2**, **XBK_BAR.2.1** and **XBK_BAR.2.2** requirements.

O7 – Databases and Operating Systems Integrity

Again this security objective is satisfied by cryptographic functions for protecting communications links, user data, configuration information and audit information: **FCS_CKM.1.1_2**, **FCS_CKM.2.1**, **FCS_COP.1.1_6**, **FCS_COP.1.1_7** and **FCS_COP.1.1_8**.

The prevention of the modifications to the audit database is implemented by the **XAA_RAR.1.1** requirement.

O8 – Authentication & Accountability of environment computing resources

Again this security objective is satisfied by cryptographic functions for protecting communications links, user data, configuration information and audit information: **FCS_CKM.1.1_2**, **FCS_CKM.2.1**, **FCS_COP.1.1_6**, **FCS_COP.1.1_7**, **FCS_COP.1.1_8**, and **FCS_CKM.4.1** requirements.

The authentication of "static" data (not data that is being transferred) is implemented by the **FDP_DAU.1.1** and **FDP_DAU.2.1** requirements.

The authentication mechanisms in order to access the certificates signing keys are implemented by the following requirements: **FCS_CKM.1.2**, **FCS_CKM.3.2**, **FCS_CKM.1.3**, **FCS_CKM.4.2** and **FCS_CKP.1.1**.

The authentication mechanisms in order to access the infrastructure and control keys are implemented by the following requirements: **FCS_CKM.1.2, FCS_CKM.3.2** and **FCS_CKP.1.1.**

The authentication mechanisms in order to access the secret/private keys are implemented by the **FCS_CKM.4.3, FCS_CKP.2.1, FCS_CKP.2.2** and **FCS_CKP.1.1** requirements.

The authentication mechanisms in order to prevent interception in public keys that have not been certified are implemented by the **FCS_CKP.1.1** requirement.

The authentication mechanisms applied to the certification requests are implemented by the **XCG_CGE.1.1** and **XTS_REC.1.1** requirements.

The authentication mechanisms applied to the revocation of certificates signing keys are implemented by the **XRM_CSC.1.3** requirement.

The authentication mechanisms applied to periodical messages provided by the Revocation Status Service (only must come from trusted Revocation Management Services) are implemented by the **XRS_RSD.1.1** requirement.

The authentication mechanisms applied to the generation of backups and recovery of the system are implemented by the **XBK_BAR.1.2** and **XBK_BAR.2.2** requirements.

O9 – Confidentiality of security services

Again this security objective is satisfied by cryptographic functions for protecting communications links, user data, configuration information and audit information: **FCS_CKM.1.1_2**, **FCS_CKM.2.1**, **FCS_COP.1.1_6**, **FCS_COP.1.1_7**, **FCS_COP.1.1_8**, and **FCS_CKM.4.1** requirements.

The confidentiality mechanisms applied to the certificates signing keys are implemented by the following requirements: **FCS_CKM.1.2**, **FCS_CKM.1.3, FCS_CKM.3.2**, **FCS_CKM.4.2** and **FCS_CKM.4.3.**

The confidentiality mechanisms applied to the secret/private keys are implemented by the **FCS_CKP.2.2** requirement.

The confidentiality mechanisms applied to the infrastructure and control keys are implemented by the **FCS_CKP.3.1** requirement.

The confidentiality mechanisms applied to the Subscriber information are implemented by the **XR_SDM.1.1** requirement.

The confidentiality mechanisms applied to the TSA signing keys and TSA control keys are implemented by the **XTS_REG.2.2** requirement.



Dependency rationale

Functional and Assurance Requirements Dependencies

The functional and assurance requirements dependencies are not completely fulfilled, a justification is done in the following section.

Justification of Unsatisfied Dependencies

The following security functional dependencies are not completely supported by security functional requirements in chapter 5.

SFR	Dependency not Satisfied
FCS_CKM.1	FMT_MSA.2
FCS_CKM.2	FMT_MSA.2
FCS_CKM.3	FMT_MSA.2
FCS_CKM.4	FMT_MSA.2
FCS_COP.1	FMT_MSA.2
FDP_ITT.1	FDP_ACF.1

FMT_MSA.2 and FDP_ACF.1.1 are not satisfied because there isn't any control access rule based on security attributes, but only initial authentication to the TOE applications is implemented based on digital certificates. Once a user has been identified and authenticated to the application at the startup, no more access control is required to access application data and functions.

TOE Summary Specification Rationale

Justification of functional requirements

How specific IT Security Functions work together so as to satisfy TOE security Functional requirements are completely described in chapter 6.

The use of extended functional requirements are justified to meet specific security requirements for Certificate Service Providers claiming conformance with [CEN01c]. They are based on the requirements in the [Èur99b], and are implemented for covering the set of rules, procedures, practices, or guidelines imposed by [CEN01c] upon Certificate Service Providers operations, providing mandatory and supplementary functionality focused on PKI standards and protocols.



Justification of assurance requirements compliance with the stated assurance measures

The justification that stated assurance measures are compliant with all the assurance requirements for EAL2 are also demonstrated in the chapter 6.

Justification on strength of functions

The assertion of Strength of Functions is determined by the assurance package level EAL2 as basic. A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential. This qualification is expressing the minimum efforts assumed necessary to defeat TOE expected security behaviour by directly attacking its underlying security mechanisms.

Only the functions that are supported by security cryptographic mechanisms require a degree of strength. The [K121STRENGTHFUNC] document comprises a relation of documents, standards an key sizes employed by different PKI functions.

Rationale for Extensions

The following set of requirements doesn't fit exactly in any of the CC Part 2 requirements nor CC part 3, so extended requirements have been defined for these main reasons:

a) the TOE contains security functionality unique to that TOE, due to the particular security properties required in public key infrastructures which are mainly focused in achieving trust and reliability;

b) there are security requirement which could be translated, but only with great difficulty and/or complexity based on security requirements components in CC Part 2 and/or Part 3.

Rationale that Requirements are Mutually Supportive

The requirements represented in this PP were developed from a variety of sources. The security work mutually so that each SFR is protected against bypassing, tampering, deactivation, and detection attacks by other SFRs.

Bypass

Prevention of bypass is derived as described below:

FIA_UID.1 and FIA_UAU.1 support other functions' allowing user access to data by limiting the actions the user can take prior to identification and authentication.



The management functions, including FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1 support all other SFRs by restricting the ability to change certain management functions to certain specified roles, thus ensuring that other users cannot circumvent these SFRs.

Tamper

Prevention of tamper is derived as described below:

FAU_STG.1 protects the integrity of the audit trail.

FCS_CKM.1 and FCS_COP.1 provide for the secure generation and handling of keys, and therefore support those SFRs that may rely on the use of those keys.

FIA_UID.1 and FIA_UAU.1 support other functions allowing user access to data by limiting the actions the user can take prior to identification and authentication.

Deactivation

Prevention of deactivation is derived as described below:

The access control SFP detailed in FDP_ACF.1 along with the other SFRs dealing with access control, provide for rigorous control of allowed data manipulations and thus prevent unauthorized deactivation.

The management functions, including FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1, support all other SFRs by restricting the ability to change certain management functions to certain specified roles, thus ensuring that other users cannot circumvent these SFRs.

FPT_TST_CIMC.2 provides for integrity testing to ensure that selected security functions are operational, thus checking for tampering. FMT_MSA.2 (Security Levels 2-4) and FMT_MSA.3 limit the acceptable values for secure data, thus providing protection from deactivation to those SFRs dependent on that data.

Detection

Detection is derived as described below:

The security audit functions, including FAU_GEN.1, FAU_GEN.2, and FAU_SEL.1 provide for the generation of audit data that may be used to detect attempts to defeat specific SFRs or potential misconfiguration that could leave the TOE prone to attack.

FAU_SAR.1 and FAU_SAR.3, support the audit generation SFRs by providing the capability to selectively search the audit records.

FAU_STG.1, and FAU_STG.4 provide for the protection of the audit records.

Extended Security Functional Requirements

Class FPT: Protection of the TSF

This class contains families of functional requirements that relate to the integrity and management of the mechanisms that provide the TSF (independent of TSP-specifics) and to the integrity of TSF data (independent of the specific contents of the TSP data).

The Protection of the TSF Class decomposition is the one included in the Common Criteria Security Functional Requirements document, where the FPT_STM Time Stamps family has been modified in order to include the FPT_STM.2 Time Synchronization component.

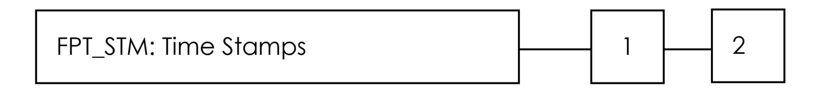


Figure 8-1: Modification of the "Protection of the TSF" Class decomposition

Time Stamps (FPT_STM)

Family Behaviour

This family addresses requirements for a reliable time stamp function within a TOE.

Component leveling



FPT_STM.1, Reliable time stamps, requires that the TSF provide reliable time stamps for TSF functions.

At FPT_STM.2, the TSF shall introduce instructions and requirements related to the reliable obtaining of the time, at the CSP services that are time dependant.

Management: FPT_STM.1, FPT_STM.2

The following actions could be considered for the management functions in FMT:

a) Management of the time

Audit: FPT_STM.1

The following actions should be auditable if FAU_GEN Security Audit data generation is included in the PP/ST :

a) Minimal: changes to the time;

b) Detailed: providing a timestamp.

Audit: FPT_STM.2

There are no auditable events foreseen.



FPT_STM.2 Time Synchronization

FPT_STM.2.1:

The TSF shall ensure that all the clocks of TWSs used for delivering CSP services that are time dependant are synchronized to within the following metric [assignment: *a defined synchronization metric*].

Class FCS: Cryptographic support

The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel and data separation. This class is used when the TOE implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software.

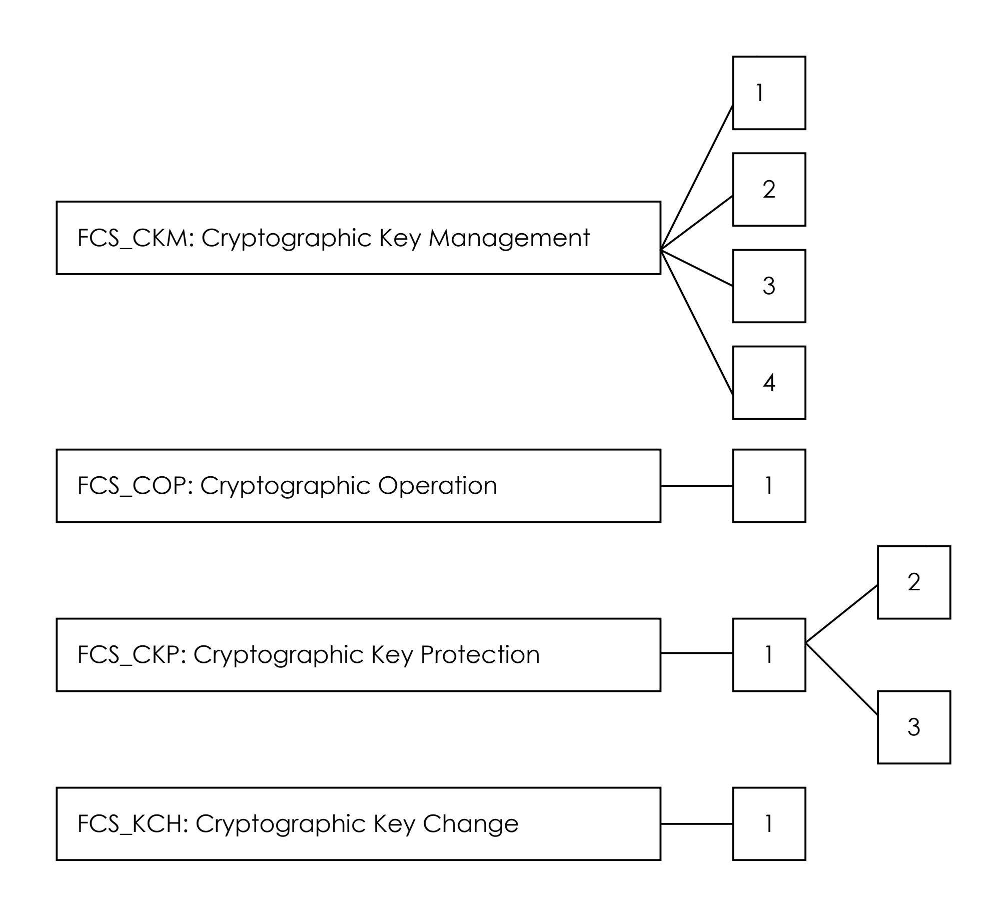


Figure 8-2: Modification of the "Cryptographic support" Class decomposition

The Cryptographic support Class decomposition is the one included in the Common Criteria Security Functional Requirements document, with the following modifications:

- The FCS_CKM Cryptographic key management family has been modified in order to include inside the FCS_CKM.1 Cryptographic key generation component, the FCS_CKM.1.2 and FCS_CKM.1.3 new requirements.

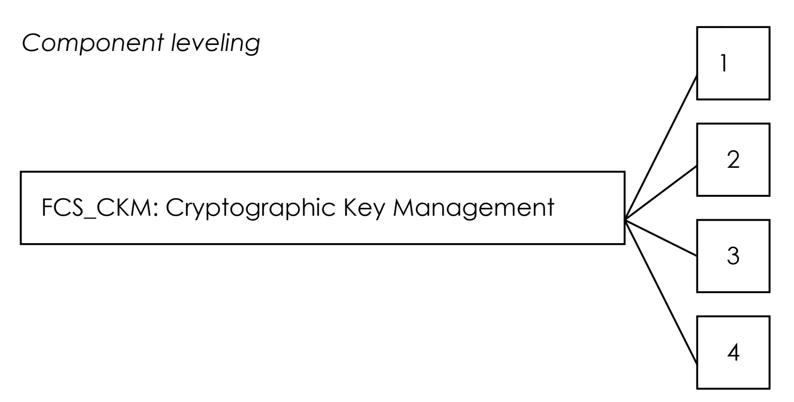
- The FCS_CKM Cryptographic key management family has been modified in order to include inside the FCS_CKM.4 Cryptographic key destruction component, the FCS_CKM.4.2 and FCS_CKM.4.3 new requirements.
- The FCS_CKP Cryptographic Key Protection new family has been created.
- The FCS_KCH Cryptographic Key Change new family has been created.

Cryptographic Key Management (FCS_CKM)

Family Behaviour

Cryptographic keys must be managed throughout their life cycle. This family is intended to support that lifecycle and consequently defines requirements for the following activities: cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction. This family should be included whenever there are functional requirements for the management of cryptographic keys.

Component leveling



FCS_CKM.1 Cryptographic key generation, requires cryptographic keys to be generated in accordance with a specified algorithm and key sizes which can be based on an assigned standard. This component also requires security conditions under which cryptographic keys are generated. Due to the different threats on the keys of TWSs, depending upon where and how they are used, it is important to categorize keys according to their risk profile. For this specification, keys are separated into the following categories:

- QC/NQC Signing Keys - Certificate Generation Service's key pair for producing Qualified Certificates or Non-Qualified Certificates and keys for signing certificate status information;
- Infrastructure Keys – these are keys used by the TWSs for processes such as key agreement, subsystem authentication, audit log signing, encrypting transmitted or stored data, etc. Short term session keys are not categorised as Infrastructure keys;
- TWS Control Keys – these are keys used by personnel managing or using the TWS and may provide authentication, signing or confidentiality services for personnel interacting with the system.

In terms of security requirements, QC/NQC Signing Keys are long-term keys whose impact from exposure is high. Consequently, countermeasures for managing this



risk are also high, both in number and in effect. Infrastructure keys are also considered high risk but due to their distributed functionality and shorter lifespan they are a lower risk in comparison to signing keys. The lowest risk keys, used by CSP TWSs, are considered to be those used by personnel for controlling TWSs, as these are used by trusted individuals and have an even shorter lifespan. Session keys, used for single/short transactions are treated as sensitive information but with lower security requirements to the above stated categories.

Infrastructure and Control keys may be either asymmetric or symmetric keys.

FCS_CKM.2 Cryptographic key distribution, requires cryptographic keys to be distributed in accordance with a specific distribution method which can be based on an assigned standard.

FCS_CKM.3 Cryptographic key access, requires access to cryptographic keys to be performed in accordance with a specific access method which can be based on an assigned standard, and property protection of these keys.

FCS_CKM.4 Cryptographic key destruction, requires cryptographic keys to be destroyed in accordance with a specific destruction method which can be based on an assigned standard. This component also requires that the TSF enforces the appropriate functions in order to destroy a compromised key or a key that reaches the end of its operational life, in order to prevent any further used of the key.

Management: FCS_CKM.1 FCS_CKM.2 FCS_CKM.3 FCS_CKM.4

The following actions could be considered for the management functions in FMT:

a) The management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).

Audit: FCS_CKM.1 FCS_CKM.2 FCS_CKM.3 FCS_CKM.4

The following actions should be auditable if FAU_GEN Security Audit data generation is included in the PP/ST :

a) Minimal: Success and failure of the activity.

b) Basic: the object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

FCS_CKM.1 Cryptographic key generation

Dependences: (One of the following: FCS_CKM.2 Cryptographic key destruction FCS_COP.1 Cryptographic operation) FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

FCS_CKM.1.2:

The TSF shall ensure that the specified key types [assignment: *list of cryptographic key types*] MUST be generated and stored in a hardware cryptographic device.

FCS_CKM.1.3:

The TSF shall ensure that the secure cryptographic module ONLY generates the specified key types [assignment: *list of cryptographic key types*] when the following conditions occurs [assignment: *list of conditions under which key generation is required*].

FCS_CKM.3 Cryptographic key access

Dependences: (One of the following: FDP_ITC.1 Import of user data without security attributes FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

FCS_CKM.3.2:

The TSF shall ensure access controls in place for all secure cryptographic modules used for the specified key types [assignment: *list of cryptographic key types*].

FCS_CKM.4 Cryptographic key destruction

Dependences: (One of the following: FDP_ITC.1 Import of user data without security attributes FCS_CKM.1 Cryptographic key generation) FMT_MSA.2 Secure security attributes

FCS_CKM.4.2:

The TSF shall ensure that the specified key types [assignment: *list of cryptographic key types*] are destroyed when the following conditions occurs [assignment: *list of conditions under which key destruction is required*] such that the signing keys cannot be retrieved.

FCS_CKM.4.3:

The TSF shall ensure that systems have been used to generate, use or store the specified key types [assignment: *list of cryptographic key types*] and are to be withdrawn from service or transferred their associated keys MUST be destroyed.

Cryptographic Key Protection (FCS_CKP)

Family Behaviour

The TSF shall introduce functions security requirements in order to protect and securely distribute the Certificate Generation Service's QC/NQC public key, Infrastructure or Control keys. Due to the different threats on the keys of TWSs, depending upon where and how they are used, it is important to categorize keys according to their risk profile. For this specification, keys are separated into the following categories:

- QC/NQC Signing Keys - Certificate Generation Service's key pair for producing Qualified Certificates or Non-Qualified Certificates and keys for signing certificate status information;
- Infrastructure Keys – these are keys used by the TWSs for processes such as key agreement, subsystem authentication, audit log signing, encrypting transmitted or stored data, etc. Short term session keys are not categorised as Infrastructure keys;

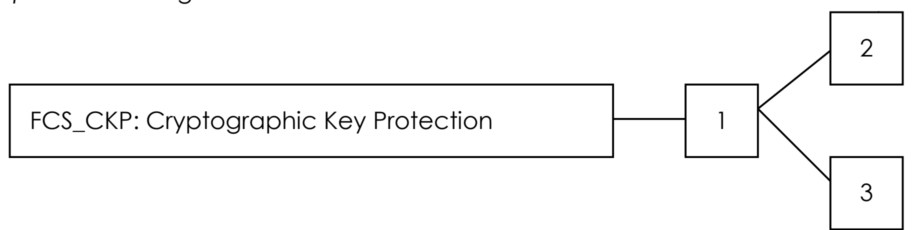


- TWS Control Keys – these are keys used by personnel managing or using the TWS and may provide authentication, signing or confidentiality services for personnel interacting with the system.

In terms of security requirements, QC/NQC Signing Keys are long-term keys whose impact from exposure is high. Consequently, countermeasures for managing this risk are also high, both in number and in effect. Infrastructure keys are also considered high risk but due to their distributed functionality and shorter lifespan they are a lower risk in comparison to signing keys. The lowest risk keys, used by CSP TWSs, are considered to be those used by personnel for controlling TWSs, as these are used by trusted individuals and have an even shorter lifespan. Session keys, used for single/short transactions are treated as sensitive information but with lower security requirements to the above stated categories.

Infrastructure and Control keys may be either asymmetric or symmetric keys.

Component leveling



FCS_CKP.1 Security mechanisms applied to cryptographic keys, requires the protection of the Certificate Generation Service's QC/NQC public key, Infrastructure, Control keys or Subject keys.

FCS_CKP.2 Protection in Key Distribution, requires the protection in the key distribution of the Certificate Generation Service's QC/NQC public key, Infrastructure or Control keys, and security mechanisms applied to the exportation of key material.

At FCS_CKP.3 Key Storage, Backup and Restore, requires that the TSF enforces the appropriate functions in order to backups up the keys and recovery following an specified method.

Management: FCS_CKP.1 FCS_CKP.2 FCS_CKP.3

The following actions could be considered for the management functions in FMT:

a) The management of changes to cryptographic key attributes.

Audit: FCS_CKP.1 FCS_CKP.2 FCS_CKP.3

The following actions should be auditable if FAU_GEN Security Audit data generation is included in the PP/ST :

a) Minimal: Success and failure of the activity.

FCS_CKP.1 Security mechanisms applied to cryptographic keys

Dependences: FCS_CKM.1 Cryptographic Key Generation FCS_XKM.4 Cryptographic Key Destruction FCS_CKM.3 Cryptographic key access



FCS_CKP.1.1:

The TSF shall be able to [selection, choose one of: *prevent, detect*] interception or manipulation in public keys that have not been certified.

FCS_CKP.1.2:

The TSF shall ensure that does not exist functions that allow for [selection: *backup, escrow*] of the specified key types [assignment: *list of cryptographic key types*].

FCS_CKP.1.3:

The TSF shall ensure that does not exist functions that allow archiving of the specified key types [assignment: *list of cryptographic key types*].

FCS_CKP.2 Protection in key distribution

Dependences: FCS_CKM.1 Cryptographic Key Generation FCS_XKM.4 Cryptographic Key Destruction FCS_CKM.3 Cryptographic key access

FCS_CKP.2.1:

The TSF shall not distribute in plain text the specified key types [assignment: *list of cryptographic key types*].

FCS_CKP.2.2:

The TSF shall ensure that any sensitive key material SHALL never be stored in an unprotected state. If the specified key types [assignment: *list of cryptographic key types*] are exported form the module where they are stored, the these keys MUST be protected by this module, to ensure its confidentiality, before being stored outside that module. If the specified key types are protected by encryption, then the TSF shall encrypt these keys in accordance with a specified cryptographic algorithm that meet the following [assignment: *list of standards*].

FCS_CKP.3 Key Storage, Backup and Restore

Dependences: FCS_CKM.1 Cryptographic Key Generation FCS_XKM.4 Cryptographic Key Destruction FCS_CKM.3 Cryptographic key access

FCS_CKP.3.1:

The TSF shall ensure that the specified key types [assignment: *list of cryptographic key types*] MUST be stored using a specified secure storage mechanism [assignment: *list of storage mechanisms*].

FCS_CKP.3.2:

The TSF shall ensure that the backup, storage and restoration of the specified key types [assignment: *list of cryptographic key types*] is only performed by [assignment: *users*] when the following conditions occur [assignment: *list of conditions under which backup, storage and restoration are required*].



Cryptographic Key Change (FCS_KCH)

Family Behaviour

A CSP operating TWSs needs guarantees and security requirements regarding to the key change. The key change may be:

- Programmed – where a key is replaced by a newly generated key once it reaches the end of its operational life (as determined by policy).
- Non- Programmed – where a key is replaced by a newly generated key if it has been compromised.

Component leveling



FCS_KCH1 Key Change Guarantees, requires mechanism in order to change keys in a secure manner.

Management: FCS_KCH.1

The following actions could be considered for the management functions in FMT:

a) The management of changes to cryptographic key attributes.

Audit: FCS_KCH.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of the activity.

FCS_KCH.1 Key Change Guarantees

Dependences: FCS_CKM.1 Cryptographic Key Generation FCS_XKM.4 Cryptographic Key Destruction FCS_CKM.3 Cryptographic key access

FCS_KCH.1.1:

The TSF shall ensure that the specified key types [assignment: *list of cryptographic key types*] SHOULD be changed on a regular basis, e.g. annually.

FCS_KCH.1.2:

The TSF shall ensure that the changeover MUST be carried out securely and MAY be an online or an out-of-band change.

Class FCO: Communication

This class provides two families specifically concerned with assuring the identity of a party participating in a data exchange. These families are related to assuring the identity of the originator of transmitted information (proof of origin) and assuring the identity of the recipient of transmitted information (proof of receipt). These families

ensure that an originator cannot deny having sent the message, nor can the recipient deny having received it.

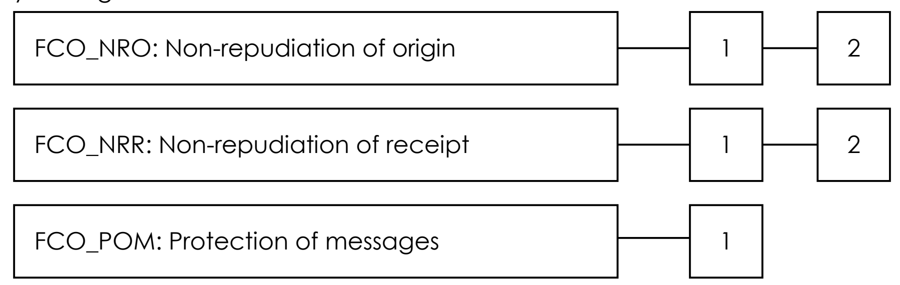


Figure 8-3: Modification of the "Communication" Class decomposition

The Commuication Class decomposition is the one included in the Common Criteria Security Functional Requirements document, with the following modifications:

- The FCO_POM Protection of messages new family has been created.

Protection of messages (FCO_POM)

Family Behaviour

This family defines the rules for detecting modification of TSF data during transmission and protects TSF data from authorized disclosure.

This family consists on only one component, FCO_POM.1 Protection of messages created by core services, which requires that the TSF shall be able to avoid the replay attack, and that the TSF provide reliable time stamps for TSF functions.

Component leveling



At FCO_POM.1, the TSF shall introduce restrictions about the protection of TSF data during transmission between different components of the TSF.

Management: FCO_POM.1

The following actions could be considered for the management functions in FMT:

a) Management of the time.

b) Management of the types of action that the TSF could take if TSF data is modified in transit.

Audit: FCO_POM.1

The following actions should be auditable if FAU_GEN Security Audit data generation is included in the PP/ST :

a) Minimal: Success and failure of the activity.

b) Minimal: The detection of modification of transmitted TSF data.



c) Basic: The action taken upon detection of modification of transmitted TSF data.

FCO_POM.1 Protection of messages created by core services

Dependences: FCS_CKM.1 Cryptographic Key Generation FCS_COP.1 Cryptographic Key Operation FPT_STM.2 Time Synchronization

FCO_POM.1.1:

The TSF shall ensure that the specified messages created by core services [assignment: *list of messages where the protection is applied*] are protected by using the service's infrastructure keys, contain a message time to indicate the time at which the sender created the message, and they include replay attack protection.

Class XR: Registration Service

This class provides two families that support the security requirements necessary by a Registration Service. The Registration Service verifies the identity and, if applicable, any specific attributes of a Subject. The results of this service are passed to the Certificate Generation Service. The families included in this class support the availability of required security mechanisms such as the protection of the certification request, or the protection of the subject data.

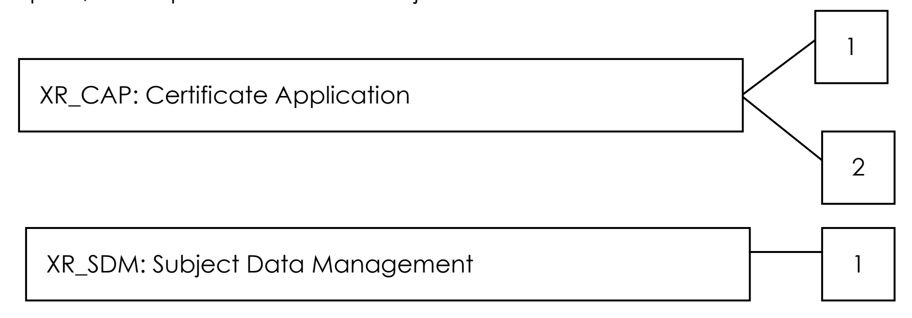


Figure 8-4: Registration Service Class decomposition

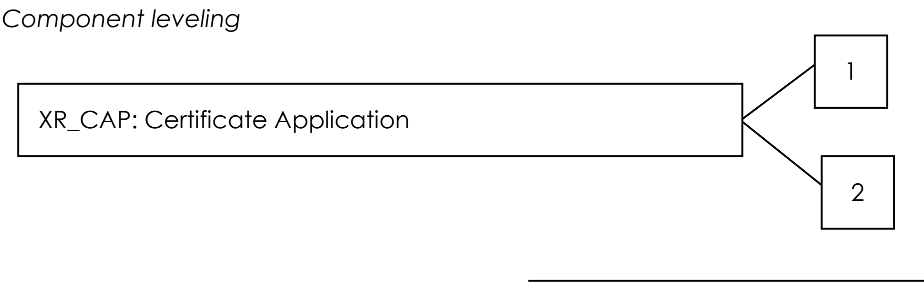
Certificate Application (XR_CAP)

Family Behaviour

This family defines security requirements applied to the Certificate Application, such as the protection mechanisms used in the certification requests, or the collection of data obtained by this Certification Application.

A Registration Officer verifies by appropriate means, in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a NQC/QC is issued.

Component leveling



At XR_CAP.1, the TSF shall introduce restrictions about the protection of the Certification Request.

At XR_CAP.2, the TSF shall introduce the requirements regarding to the data that the Certificate Application must collected.

Management: XR_CAP.1

The following actions could be considered for the management functions in FMT:

a) Management of the types of action that the TSF could take if TSF data are modified in transit.

Management: XR_CAP.2

There are no management activities foreseen.

Audit: XR_CAP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Successful transfers of user data, including identification of the integrity protection method used.

b) Minimal: The identity of any user or subject using the data exchange mechanisms.

c) Basic: Unauthorized attempts to change the integrity protection method.

d) Detailed: The action taken upon detection of an integrity error.

Audit: XR_CAP.2

There are no auditable events foreseen.

XR_CAP.1 Protection of the Certification Request

Dependencies: FCS_CKM.1 Cryptographic Key Generation FCS_COP.1 Cryptographic Key Operation FDP_DAU.2 Data Authentication with Identity of Guarantor

XR_CAP.1.1:

The TSF shall ensure that the Certificate Requests MUST be protected before being forwarded from the Registration Service to the Certification Generation Service, thus ensuring [selection: *message confidentiality, authentication, data integrity*], by using the specified key types [assignment: *list of cryptographic key types*].

XR_CAP.1.2:

The TSF shall provide a mechanism to allow approval of certificate applications, by [assignment: *authorized users*], before leaving the Registration Service.



XR_CAP.2 Collection of User Data

XR_CAP.2.1:

The TSF shall ensure that the Registration Service MUST be configured to allow collection of enough data from the subject to satisfy the requirements for Qualified Certificates according to the following [assignment: *list of standards*]

Subject Data Management (XR_SDM)

Family Behaviour

This family defines security requirements necessary to protect the Subject information.

Component leveling



At XR_SDM.1, the TSF shall introduce requirements necessary to protect the subject information.

Management: XR_SDM.1

There are no management activities foreseen.

Audit: XR_SDM.1

There are no auditable events foreseen.

XR_SDM.1 Subject Data Management

XR_SDM.1.1:

The TSF shall ensure that the ability to implement mechanisms and security controls to protect the privacy and confidentially of Subject information.

Class XCG: Certificate Generation Service

This class in intended to specify the management of several aspects of the Certificate Generation Service. This service creates and signs certificates based on the identity and other attributes of a Subject as verified by the Registration Service.

This class provides two families that support the processes related to the Certificate Generation, and the functional requirements associated with the Certificate Renewal.

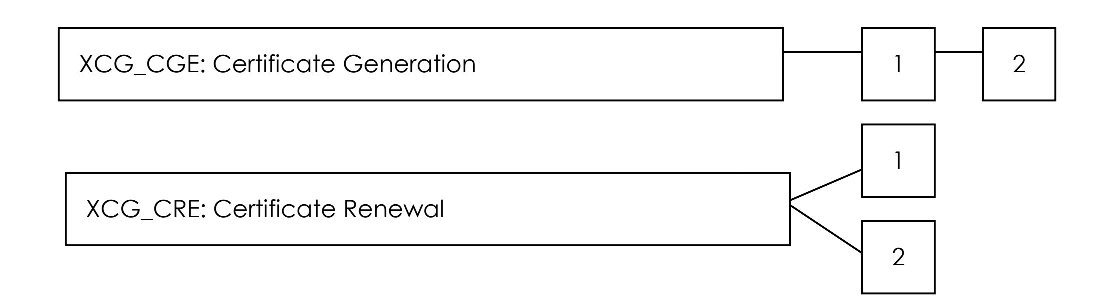


Figure 8-5: Certificate Generation Service Class decomposition

Certificate Generation (XCG_CGE)

Family Behaviour

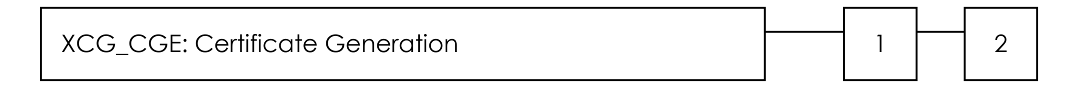
This family defines security requirements applied to the certificate generation. After receiving a certificate application from the Registration Service, TWSs generate a certificate using the public key supplied. This ensures the CSP has "locked" the binding of the Subject's public key to its identity.

TWSs may also send their Infrastructure or Control Public Keys to be certified by the Certificate Generation Service. This produces Infrastructure or Control Certificates.

Following Certificate Generation, the certificate may be made available via the supplementary Subject Device Provision or to the Subject directly.

Infrastructure and Control Certificates may be provided directly to the trustworthy component requiring its use.

Component leveling



At XCG_CGE.1, the TSF shall introduce security requirements about the process of the certification request

At XCG_CGE.2, the TSF shall introduce guarantees and properties related to the issued certificates.

Management: XCG_CGE.1

The following actions could be considered for the management functions in FMT:

a) The management (deletion, modification, addition) of the actions related to the maintenance of the Certificate Policy.

b) Management of the types of action that the TSF could take if the Certification Request is modified in transit.

Management: XCG_CGE.2



The following actions could be considered for the management functions in FMT:

a) The management of changes to cryptographic key attributes.

Audit: XCG_CGE.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success of failure of the certificate generation.

b) Minimal: Changes in the Certificate Policy data.

c) Minimal: Successful transfers of the Certification Request, including identification of the integrity protection method used.

d) Minimal: The identity of any user using the Certification Request Process.

e) Basic: Unauthorized attempts to change the integrity protection method in a Certification Request.

f) Detailed: The action taken upon detection of an integrity error in a Certification Request

Audit: XCG_CGE.2

There are no auditable events foreseen.

XCG_CGE.1 Process of the Certification Request

Dependencies: FCS_CKM.1 Cryptographic Key Generation FCS_COP.1 Cryptographic Key Operation FCS_CKM.3 Cryptographic key access

XCG_CGE.1.1:

The TSF shall ensure that the Certificate Generation Service MUST ensure the [selection: *integrity, data origin authenticity, privacy and confidentiality*] of the certificate request message.

XCG_CGE.1.2:

The TSF shall provide a mechanism to allow the certificate request was processed securely and checked for conformance with the applicable Certificate Policy.

XCG_CGE.1.3:

The TSF shall ensure that before certificate generation, the TWS MUST ensure Proof of Possession is validated.

XCG_CGE.2 Guarantees of the issued certificates

Dependencies: FCS_CKM.1 Cryptographic Key Generation FCS_COP.1 Cryptographic Key Operation FCS_CKM.3 Cryptographic key access XKM_SBA.1 Key Storage FCS_CKP.2 Protection in key distribution FCS_CKP.3 Key Storage, Backup and Restore

XCG_CGE.2.1:

The TSF shall ensure that the key used to sign a Qualified Certificate should only be used for signing Qualified Certificates and, optionally the related Revocation Status Data.

XCG_CGE.2.2:

The TSF shall ensure that the certificates issued by the TWS MUST have the following properties [assignment: *properties that must include the certificates*].

XCG_CGE.2.3:

The TSF shall ensure that the Qualified Certificates issued by the TWS MUST conform to the following: [assignment: *list of standards*].

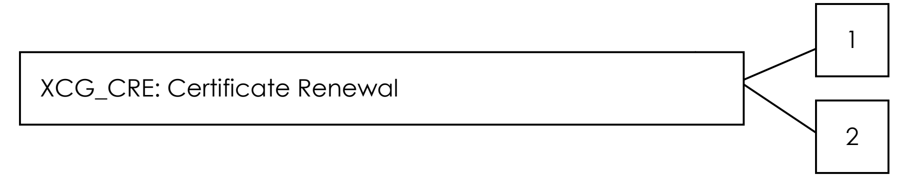
Certificate Renewal (XCG_CRE)

Family Behaviour

This family defines security requirements applied to the certificate renewal. During the period prior to the expiration of the certificate, such period being defined by applicable policy, the certificate may be renewed. The Certificate renewal may consist of a Re-key scenario: a new public key is certified using the registration information used to generate the previous certificate.

Certificate renewal covers QC/NQC Signature, Infrastructure, Control and Subject Certificate.

Component leveling



At XCG_CRE.1, the TSF shall introduce security requirements about the certificate renewal process of QC/NQC Signature, Infrastructure, and Control certificates.

At XCG_CRE.2, the TSF shall introduce security requirements about the certificate renewal process of Subject certificates.

Management: XCG_CGE.1 XCG_CGE.2

The following actions could be considered for the management functions in FMT:

a) The management of changes to cryptographic key attributes.

Audit: XCG_CGE.1 XCG_CGE.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of the activity.



XCG_CRE.1 Certificate Renewal in non-Subject entities

Dependencies: FCS_CKM.1 Cryptographic Key Generation

XCG_CRE.1.1

The TSF shall ensure that the specified key types [assignment: *list of cryptographic key types*] are updated prior to their expiry, with the following conditions [assignment: *list of conditions under which key update is required*].

XCG_CRE.2 Certificate Renewal in Subject entities

Dependencies: FCS_CKM.1 Cryptographic Key Generation

XCG_CRE.2.1

The TSF shall ensure that the mechanism used for [selection, choose one of: *re-keying, re-certifying*] of Subject keys accomplishes with the following conditions [assignment: *list of conditions under which key renewal is required*].

Class XRM: Certificate Revocation Management Service

This class in intended to specify the management of several aspects of the Revocation Management Service and the Revocation Status Service.

The Revocation Management Service is in charge of process requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the Revocation Status Service.

The Revocation Status Service provides certificate revocation status information to relying parties. This service may be a real-time service or may be based on revocation status information which is updated at regular intervals.

This class provides two families that support the processes related to the Certificate Status Change Requests, and the processes related to Certification Revocation/Suspension.

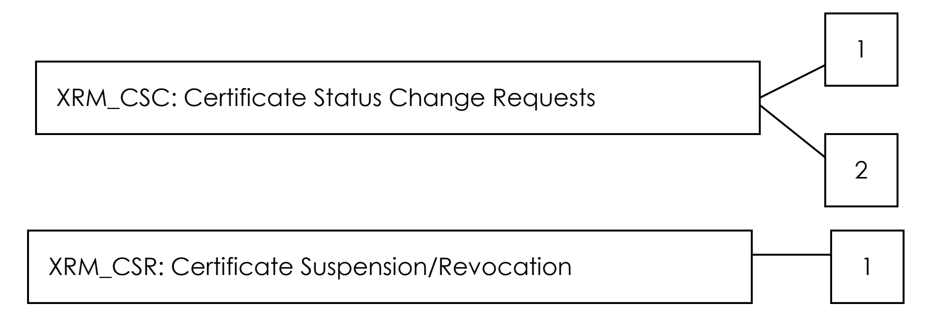


Figure 8-6: Certificate Revocation Management Service Class decomposition

Certificate Status Change Requests (XRM_CSC)

Family Behaviour

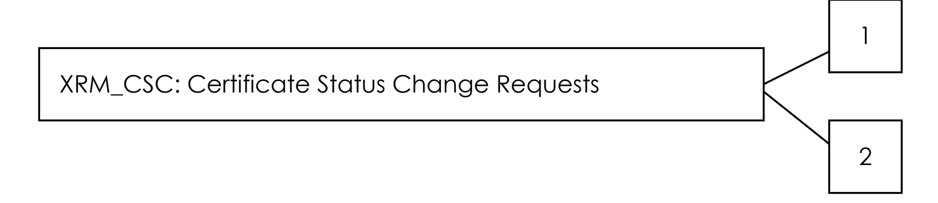
This family defines security requirements applied to the certificate status change requests. Where a Subject determines that their private key may be compromised, a

request for suspension (temporally revocation) of their certificate is sent to their CSP's TWS. A corresponding request to restore a certificate from suspension to operational use may be made by the Subject.

Where the Subject knows that the private key is compromised, a request for revocation of their certificate is sent to their CSP's TWS.

The CSP may also request a certificate status change via this service. Status of Control and Infrastructure Certificates may also be controlled through this service. Requests for certificate status change are authenticated messages and may be accepted or rejected by the CSP.

Component leveling



At XRM_CSC.1, the TSF shall introduce security requirements about the process of the certification status change request.

At XRM_CSC.2 requires actions to perform after request/report processing is complete.

Management: XRM_CSC.1

The following actions could be considered for the management functions in FMT:

a) The management of changes to cryptographic key attributes

b) Management of the types of action that the TSF could take if TSF data is modified in transit.

Management: XRM_CSC.2

There are no management activities foreseen.

Audit: XRM_CSC.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success of failure of the certificate generation.

b) Minimal: Successful transfers of the Revocation Request, including identification of the integrity protection method used.

c) Minimal: The identity of any user using the Revocation Request Process.

d) Basic: Unauthorized attempts to change the integrity protection method in a Revocation Request.

e) Detailed: The action taken upon detection of an integrity error in a Revocation Request.



Audit: XRM_CSC.2

There are no auditable events foreseen.

XRM_CSC.1 Security Requirements for Revocation Requests

Dependencies: FCS_CKM.1 Cryptographic Key Generation FCS_COP.1 Cryptographic Key Operation FCS_CKM.3 Cryptographic key access FCO_POM.1 Protection of Messages created by core services

XRM_CSC.1.1:

The TSF shall ensure that once a certificate is definitely revoked it cannot be reinstalled.

XRM_CSC.1.2:

The TSF shall ensure that the requests for suspension, reinstalling and revocation MUST be suitably processed when the following security conditions occur [selection: *authentication, validation*].

XRM_CSC.1.3:

The TSF shall ensure that the revocation of certificates related to QC/NQC Signing Keys MUST only be possible under the following conditions [assignment: *list of conditions under which revocation is required*].

XRM_CSC.2 Certificates Suspension/Revocation

XRM_CSC.2.1:

The TSF shall ensure that the Certificate Status database MUST be updated [assignment: *metric for updating the database]* after request/report processing is complete.

Certificate Suspension/Revocation (XRM_CSR)

Family Behaviour

This family defines security requirements applied to the certificate suspension/revocation. The TWS having obtained a suspension or revocation request via this service, changes the certificate status to either Suspended or Revoked in its Certificate Status Database, and this in turn is used by the CSP's Revocation Status Service.

A CSP is responsible for updating/providing the status of certificates on the Revocation Status Service. TWSs may implement this using:

- Periodical Messaging: where periodical update messages (e.g. CRLs/ARLs) are sent from the Revocation Management System to the Revocation Status Service or;
- Real-time Messaging: where a request/response mechanism is used and a status request via the Revocation Status Service queries the Certificate Status Database and a status response is generated and passed back via the Revocation Status Service.

Component leveling

XRM_CSR: Certificate Suspension/Revocation	1

At XRM_CSR.1, the TSF shall introduce security requirements about the update process from the Revocation Management System to the Revocation Status Service.

Management: XRM_CSR.1

The following actions could be considered for the management functions in FMT:

a) The management of changes to cryptographic key attributes

b) Management of the types of action that the TSF could take if TSF data is modified in transit.

Audit: XRM_CSR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success of failure of the certificate generation.

b) Minimal: Successful transfers of the Revocation Request, including identification of the integrity protection method used.

c) Minimal: The identity of any user using the Revocation Request Process.

d) Basic: Unauthorized attempts to change the integrity protection method in a Revocation Request.

e) Detailed: The action taken upon detection of an integrity error in a Revocation Request.

XRM_CSR.1 Update process of the Revocation Status Service

Dependencies: FCS_CKM.1 Cryptographic Key Generation FCS_COP.1 Cryptographic Key Operation FCS_CKM.3 Cryptographic Key Access XKM_SBA.1 Key Storage FPT_STM.1 Reliable Time Stamps FCO_POM.1 Protection of Messages created by core services

XRM_CSR.1.1:

The TSF shall ensure that where Periodical Messaging is used, a TWS MUST support the following requirements:

- For an offline status repository (e.g. CRL accessible through directories) the Revocation Status Service is updated at least on a daily basis.
- For an online status repository (e.g. OCSP responder) the Revocation Status Service is updated when a status change occurs and additionally at least on a daily basis.
- Each update message is include the name and digital signature of the message issuer, and the time of status change.



- The messages indicate which certificates are revoked/suspended.

For each certificate in the list, its serial number and a reason for the status change is provided in the message.

Class XRS: Certificate Revocation Status Service

This class provides two families that support the security requirements necessary by a Certificate Revocation Status Service.

The Revocation Status Service provides certificate revocation status information to relying parties. This service may be a real-time service or may be based on revocation status information which is updated at regular intervals. The Revocation Status Service shall get reliable information from the Certificate Status Database, where the Revocation Management processes insert certificate status information.

The families included in this class support the availability of required security mechanisms such as the protection of the status request/response, or the protection of the communication between the Revocation Management Process and the Revocation Status Service.

The Revocation Status Service may be an "online" servicie (providing real-time certificate status) or an "offline" service (where certificate status is not real-time).

Where this is an "online" service, a Relying Party communicates with this Revocation Status Service and provides details of the certificate(s) for which status is required. The "online" Revocation Status Service when using Real-time messaging makes a query to the Certificate Status database to retrieve the current status of the requested certificate or if using Periodical messaging queries its internal records, which have been updated by the last Periodical message. A reply is thus created and sent to the Relying Party indicating the status of the requested certificate(s). Where this is an "offline" service, the Revocation Status Service holds the most recent Periodic Message. This may be obtaining by the Relying Party for checking certificate status.

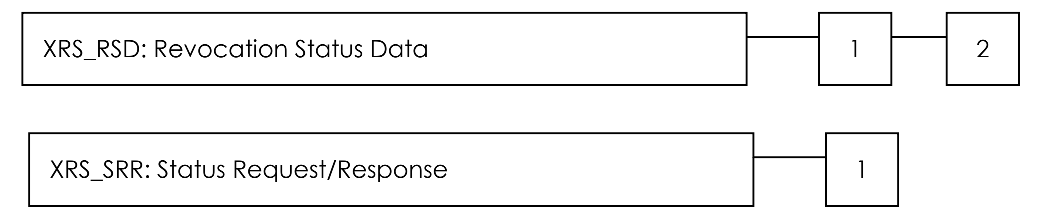


Figure 8-7: Certificate Revocation Status Class decomposition

Revocation Status Data (XRS_RSD)

Family Behaviour

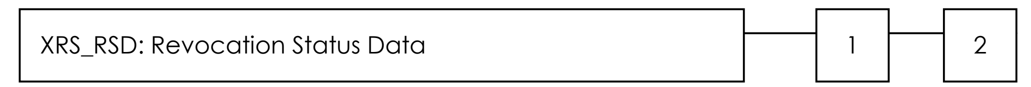
This family defines security requirements applied to the communication between the Revocation Status Service and the Revocation Management Service. This communication consists on the transfer of the certification status information from the Certificate Status Database to the Revocation Status Service.

The Revocation Status Service provides certificate revocation status information to Relying Parties. The Revocation Status Service reflects changes to certificate status,



based on status change requests either from the Subject, from the CSP, or from a third party, and processed by the Revocation Management Service. This data may also be made available to Subjects if policy requires Subjects to have access to revocation status data.

Component leveling



At XRS_RSD.1, the TSF shall introduce restrictions about the trust of the Revocation Status Service.

At XRS_RSD.2, the TSF shall introduce the requirements regarding to the security applied to the communication between the Revocation Status Service and the Revocation Management Service.

Management: XRS_RSD.1

The following actions could be considered for the management functions in FMT:

a) Maintenance (deletion, modification, addition) of the list of trusted Revocation Management Services

Management: XRS_RSD.2

The following actions could be considered for the management functions in FMT:

a) Management of the types of action that the TSF could take if TSF data is modified in transit.

b) Management of changes to cryptographic key attributes.

Audit: XRS_RSD.1

There are no auditable events foreseen.

Audit: XRS_RSD.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of the activity.

b) Minimal: The detection of modification of transmitted TSF data.

c) Basic: the action taken upon detection of modification of transmitted TSF data.

XRS_RSD.1 Trust of the Revocation Status Service

XRS_RSD.1.1:

The TSF shall ensure that [selection: *periodical messages, real-time messages*] provided by the Revocation Status Service MUST only be from trusted Revocation Management Services.



XRS_RSD.2 Communication between the Certificate Status Database and the Revocation Status Service

Dependencies: FCS_CKM.1 Cryptographic Key Generation FCS_COP.1 Cryptographic Key Operation FCO_POM.1 Protection of Messages created by core services FCS_CKM.3 Cryptographic Key Access

XRS_RSD.2.1:

The TSF shall ensure that the TWSs providing an online revocation service MUST validate the [selection: *integrity, authenticity*] of the [selection: *Periodic messages, Real-time messages*] sent to it.

Status Request/Response (XRS_SRR)

Family Behaviour

This family defines security requirements necessary to protect the Status Request/Response between a Relying Party and the Revocation Status Service.

A Relying Party having obtained the certificate(s), required for signature verification, needs to check the status of these certificates. The CSP provides a Revocation Status Service for this purpose.

TWSs may request that Relying Parties digitally sign certificate status requests. TWSs may optionally provide session confidentiality and integrity. Status requests may be generated by TWSs themselves to obtain the status of NQC/QC Signing, Infrastructure and Control Certificates.

Component leveling



At XRS_SRR.1, the TSF shall introduce requirements necessary to protect the protocol between the Relying Party and the Revocation Status Service.

Management: XRS_SRR.1

The following actions could be considered for the management functions in FMT:

a) Management of the types of action that the TSF could take if TSF data is modified in transit.

b) Management of changes to cryptographic key attributes.

Audit: XRR_SRR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of the activity.

XRS_SRR.1 Protection applied to the Status Request/Response

Dependencies: FCS_CKM.1 Cryptographic Key Generation FCS_COP.1 Cryptographic Key Operation FCS_CKM.3 Cryptographic Key Access FPT_STM.2 Time Synchronization

XRS_SRR.1.1:

The TSF shall ensure that all certificate status responses from an online Revocation Status Service MUST be digitally signed by the Revocation Status Service using [selection: *specified key type*] that meet the following [selection: *list of standards*].

XRS_SRR.1.2:

The TSF shall ensure that the response message MUST contain the time at which the Revocation Status Service/Issuer signed the response.

Class XTS: Time-Stamping Service

This class provides two families that support the security requirements necessary by a Time-Stamp Service.

A time-stamping authority (TSA) is a third party trusted to provide time-stamping services, i.e. generate time-stamp tokens, which can serve as evidence that a data item existed before a certain point in time (proof of existence).

The time-stamping service provides only a time-stamping process, which cryptographically binds time values to data values.

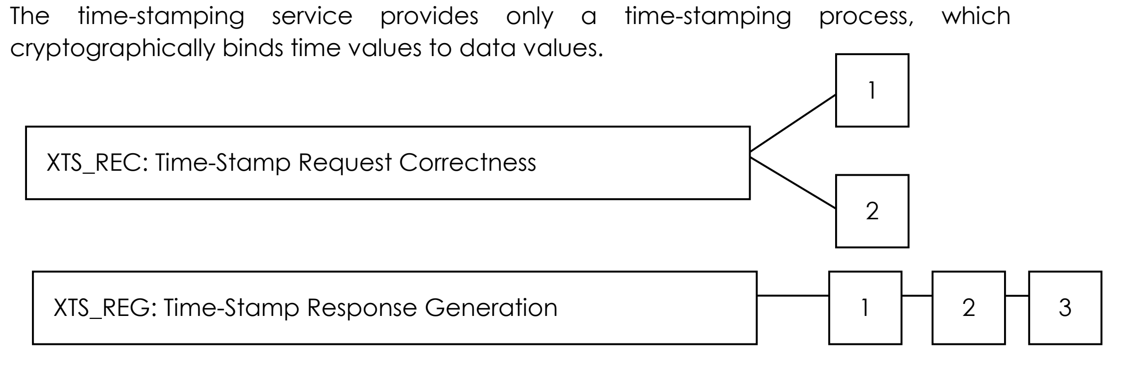


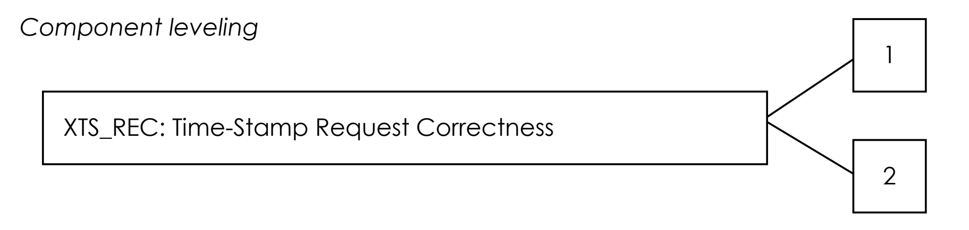
Figure 8-8: Time-Stamp Service Class decomposition

Time-Stamp Request Correctness (XTS_REC)

Family Behaviour

This family defines security requirements applied to the correctness and completeness of the request. If the result of the related functions is positive, the data item will be sent as input to the Time-Stamp Token Generation functions.

Component leveling





At XTS_REC.1, the TSF shall introduce restrictions about the verification of the origin of the request.

At XTS_REC.2, the TSF shall introduce the requirements regarding to the verification of the cryptographic algorithms used in the request.

Management: XTS_REC.1 XTS_REC.2

There are no management activities foreseen.

Audit: XTS_REC.1 XTS_REC.2

There are no auditable events foreseen.

XTS_REC.1 Verification of the origin of the request

XTS_REC.1.1:

The TSF shall provide functions in order to control the origin of each request before checking its correctness, making use of the specified security mechanisms [assignment: *method to control the origin of the request*].

XTS_REC.2 Verification of the algorithms of the request

XTS_REC.2.1:

The TSF shall ensure that the TSA verifies that the request for time-stamping, uses a hash algorithm that meet the following [assignment: *list of standards*].

Time-Stamp Response Generation (XTS_REG)

Family Behaviour

This family defines security requirements necessary to generate the Time-Stamp Response.

This family defines functions for the following purposes:

- Time Parameter Generation. These functions use a reliable source to deliver a accurate time parameters. These parameters are used as input in the Time-Stamp Generation process.
- Time-Stamp Token Generation. These functions are responsible for creating a time stamp by binding the current time, a unique serial, the data provided for time stamping and ensuring any policy requirements are adhered to.
- Time-Stamp Token Computation. These functions compute the time-stamp token that is returned to the client. It effectively cryptographically signs the data provided by the Time-Stamp Token Generation function.

Component leveling





At XTS_REG.1, the TSF shall introduce requirements necessary to include in the Time-Stamp Response a time obtained from a reliable source.

At XTS_REG.2, the TSF shall introduce requirements necessary to include data to the content of the Time-Stamp Response.

At XTS_REG.3, the TSF shall introduce requirements necessary to guarantee the security of the generated Time-Stamp Response.

Management: XTS_REG.1 XTS_REG.2

There are no management activities foreseen.

Management: XTS_REG.3

The following actions could be considered for the management functions in FMT:

a) Management of changes to cryptographic key attributes.

Audit: XTS_REG.1 XTS_REG.2

There are no auditable events foreseen.

Audit: XTS_REG.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of the activity.

XTS_REG.1 Time Parameter Generation

XTS_REG.1.1:

The TSF shall ensure that the TSA's trusted time source(s) MUST be synchronized to within the following metric [assignment: *a defined synchronization metric*].

XTS_REG.1.2:

The TSF shall ensure that the TSA's clock SHALL be synchronized with the following [assignment: *standard times reference*] using a mechanism that meet the following [assignment: *list of acceptance conditions under which the synchronization mechanism is required*].

XTS_REG.2 Content of the Time-Stamp Response

XTS_REG.2.1:

The TSF shall ensure that the Serial Number used within the TST MUST be unique for each TST issued by a given TSA. This property MUST be preserved when the following conditions occur [assignment: *list of conditions under which this property is preserved*].

XTS_REG.2.2:

The TSF shall ensure that the TST MUST include the accuracy of the time source used when the following conditions occurs [assignment: *list of conditions under which this property is preserved*].



XTS_REG.2.3:

The TSF shall ensure that an indication of the policy under which the TST was created MUST be included.

XTS_REG.2.4:

The TSF shall ensure that the TST response contains the same datum that was sent with the request.

XTS_REG.3 Security Guarantees of the Time-Stamp Response

Dependencies: XKM_KEG.1 Key Generation in a secure cryptographic device FCS_CKM.1 Cryptographic Key Generation

XTS_REG.3.1:

The TSF shall ensure that the signature algorithms/keys used by the TSA meet the following [assignment: *list of standards*].

XTS_REG.3.2:

The TSF shall ensure that the specified key types [assignment: *list of cryptographic key types*] belonging to the TSA MUST be generated and stored in a hardware cryptographic device.

Class XSP: Subject Device Provision Service

This class in intended to specify the management of several aspects of the Subject Device Provision Service. This service is considered as a CSP optional supplementary service.

The Subject Device Provision Service prepares and provides a Signature Creation Device (SCDev) to Subjects. Examples of this services are:

- A service which generates the subject's key pair and distributes the private key ti the subject,
- A service which prepares the subject's Secure Signature Creation Device (SSCD) and device enabling codes and distributes the SSCD to the registered subject.

This service may provide a SCDev and/or a SSCD. The security requirements applicable to SCDs are equally applicable to SSCDs, where SSCDs meet the additional requirements stated in Annex III of [Eur99a]. No distinction is made whether the SCDev/SSCD is implemented in hardware or software.

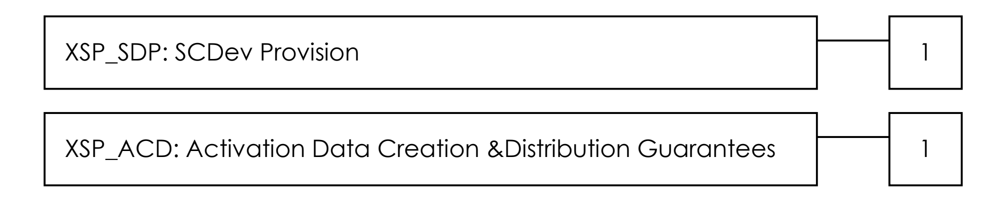


Figure 8-9: Subject Device Provision Service Class decomposition

SCDev Provision (XSP_SDP)

Family Behaviour

This family defines security requirements applied to the distribution of the SCDev (after preparation) to the Subject.

Component leveling



At XSP_SDP.1, the TSF shall introduce security requirements about the process of distribution of the SDDev to the Subject.

Management: XSP_SDP.1

There are no management activities foreseen.

Audit: XSP_SDP.1

There are no auditable events foreseen.

XSP_SDP.1 SCDev Distribution

XSP_SDP.1.1:

The TSF shall ensure through appropriate TWS configuration, that the SCDev is distributed to the intended and authenticated subject.

Activation Data Creation & Distribution (XSP_ACD)

Family Behaviour

This family defines security requirements applied to the activation data creation and distribution. The SCDev and its contents are protected with secret activation data. The CSP is responsible for generation of this initial activation data and subsequent secure distribution of this to the subject.

Component leveling



At XSP_ACD.1, the TSF shall introduce security requirements about the activation data creation and distribution processes.

Management: XSP_ACD.1

There are no management activities foreseen.

Audit: XSP_ACD.1

There are no auditable events foreseen.



XSP_ACD.1 Activation Data Creation & Distribution Guarantees

XSP_ACD.1.1

The TSF shall ensure that the [assignment: *users*] cannot misuse the SCDev at any time.

XSP_ACD.1.2

The TSF shall ensure that the initial activation data are generated in a secure manner.

Extended Security Assurance Requirements

Class XSO: Systems & Operations

This class provides two families specifically concerned with assuring the secure operation of the TWS and the reliable management of the time used by the TSF.



Figure 8-10: System & Operations Class decomposition

Operations Management (XSO_OPM)

Family Behaviour

A CSP operating TWSs needs to ensure that its operations management functions are adequately secure.

Component leveling



At XSO_OPM1, the TSF shall introduce instructions and requirements related to the TWS operations management.

Management: XSO_OPM.1

There are no management activities foreseen.

Audit: XSO_OPM.1

There are no auditable events foreseen.

XSO_OPM.1 Operations Management

Dependencies: ADO_IGS.1 Installation, generation and start-up procedures, AGD_ADM.1 Administrator guidance ADM_USR.1 User guidance

XSO_OPM.1.1:

The TWS shall provide instructions to allow the CSP system to be:

- Correctly and securely operated.
- Deployed in a manner where the risk of systems failure is minimized.

APÉNDICE A

CPS de KeyOne 2.1

The certificate policy is a set of rules governing the intended use of certificates and the level of trust that the particular Service Provider will support. The certificate policy provides the criteria that can be used by others to determine whether to trust certificates issued by the certification authority and is also the basis for accreditation of the certification authority.

The certification practice statement contains a more detailed description of the mechanics followed by a certification authority in issuing and otherwise managing certificates. It outlines the procedures used to implement the policies with regard to certificate issuance, user identification and registration, certificate lifetimes and revocation, and publishing practices for certificates and certificate revocation lists. It also states the operational practices followed by the certification authority to ensure security. The certification practices statement is used to outline operational procedures for the certification authority's personnel and also provides additional information to the relying party.

The structure of this CPS is based on the work of IIETF RFC3647 ("Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", November 2003).

Purpose of the appendix

This appendix is intended to provide a guideline for production of Certificate Policies and Certification Practice Statement to set up a Certificate Service Provider with the support of certified KeyOne 2.1 system and compliant with this Security Target. It addresses the most important issues at a high level, and the minimum requirements to take account when setting up and using the system, for matching with the evaluated configuration. The sections or issues where explicit recommendation or requirement have not been done, are only informative, and must be completed as needed by organizations. Notice that whatever change in the rest of the appendix will make the PKI system fail to match the evaluated configuration.

This appendix is structured in two main parts, the first one states certificate policy issues and second describing certificate practices.

This CPS provides factual information that describes the Practices employed to support KeyOne TWS Certificate services.

These Certificate services provide a range of security and assurance levels to support the use of Qualified Certificates created under the KeyOne PKI. End User Certificates



issued under this CA are used to digitally signed transactions and documentation legally equivalent to hand-written signatures.

Certificate services are to be considered as one of many elements in an overlapping framework of mechanisms, controls and procedures that protect and facilitate an organization's electronic business. It is critical that End Users and any other party relying upon a transaction supported by a Certificate:

1. understand the risks and threats of doing so; and,
2. ensure that appropriate mitigation and prevention measures have been put in place; and,
3. suitably position *company name*'s Certificate services within an overall risk management plan.

Certificate Policy

Certificate types issued

This CPS supports the operation of different certificate policies:

1. Qualified Certificates and Non Qualified Certificates End User which must be nominated in respective CP;
2. Infrastructure Certificates[134] issued by the KeyOne TWS:
3. Control Certificates[135] issued by KeyOne TWS CAs:

The only restrictions that certificates issued by KeyOne TWS system must fulfilled are derived from CWA [CG1.6] security requirements.

Additionally, when issuing qualified certificates, conformance with [TS101862] must be claimed.

All certificates issued by KeyOne TWS must have the following properties:

1 Indication of the subject name or pseudonym. Where a pseudonym is used this MUST be clearly indicated;

2 The public key in the certificate is related to the subject private key;

3 The advanced electronic signature of the CSP, created using the CSP Signing Keys;

4 A unique distinguished name and serial number assigned by the KeyOne TWS. This MUST be unique with respect to the issuing CSP;

---

[134] Infrastructure keys are used by the some TOE components for processes such as subsystem authentication, audit log signing, encrypting transmitted, …
[135] Control keys are used by personnel managing or using the TOE components, and that may provide authentication, signing or confidentiality services for those personnel interacting with the system.

5 The certificate SHALL specify a *valid from time* that does not precede the current time and a *valid until time* that does not precede the *valid from time*;

6 The signature algorithms/keys used by the KeyOne TWS to sign the certificate MUST be conformant to the algorithm specifications standard [ALGO];

7 Reference to the Certificate Policy under which the certificate is issued

User Community and Applicability

Certificates issued under this policy may be used to support electronic signatures which "satisfy the requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper based data", as specified in article 5.1 of Directive 1999/93/EC [Eur99b].

General Provisions

Obligations and Liabilities

Certification Authority

The user community shall be informed of the procedures for certificate registration, issuance, suspension, revocation and validation.

A Certification Authority (CA) that issues certificates must operate according to an appropriate certificate policy. The policy should as a minimum undertake to:

1 provide certification and repository services that are consistent with each other;

2 provide controls regarding operational requirements;

3 perform the authentication procedures regarding initial registration and revocation requests;

4 issue certificates in accordance with the certificate policy definition and honour the various representations to subscribers and to relying parties presented in a published CPS - Certification Practice Statement (a statement of the practices which a certification authority employs in issuing certificates);

5 support the rights of the subscribers and relying parties who use certificates in accordance with applicable laws and regulations;

6 revoke certificates and issue CRLs of the certificate policy definition (provision of certificate suspension is at the option of the certification authority); and

7 comply with all provisions of its certificate policy definition and any legal provisions in a published CPS, which esqueleton can be extracted from this appendix.



The CA is responsible for all undertakings listed above, regardless of whether they are performed by the CA or a Registration Authority (RA) appointed by the CA. CA undertakings against all external entities therefore include all RA undertakings.

CAs must provide the following additional undertakings concerning:

a) Protection of the issuing CA's private key; and

A CA should protect its private key in accordance with certain provisions described in certificate policies.

b) Restrictions on the use of the issuing CA's private key.

A CA's private key used for issuing certificates that conform to this certificate policy should be used only for signing certificates and, optionally, CRLs and other adequate information consistent with the certificate issuance.

If a CA undertakes to act in accordance with other policies, using the same private key or issuing identity, these should be identified in the CPS.

Registration Officers

Responsibilities that could be allocated to a Registration Service are:

a) validate the identity of the entity requesting a public key certificate, according to the CA's Certification Practice Statement (CPS);

b) verify the name of the entity requesting a public key certificate is unique with respect to the issuing CSP;

c) register authenticated entities securely;

d) notify the entity identified in the certificate confirming successful registration and that a certificate has been issued and publicly available, when delivering its signature creation data;

e) keep audit records supporting the certificates it issues for the length of time determined by policy requirements for retention of records, according to applicable regulations;

f) provide guidance to its subscribers on the secure management of the subscriber's private key;

g) use any appropriate means to ascertain that the entity identified in the certificate understands it's responsibilities and is able to comply with them;

h) inform the entities in the domain when the CA's private key has been compromised;

i) handle certificate revocation requests from entities;

j) inform the entity identified in the certificate that the integrity of it's operation will be considered compromised if it's private key is ever revealed to or used by any unauthorised entity; and

k) maintain sound management and control practices that are to be confirmed by security quality assurance processes and procedures, and independent compliance audits.

An RA is an entity who is responsible for identification and authentication of entities of public key certificates, but is not a CA or KEYONE TWS, and hence does not sign or issue certificates. An RA may assist in the certificate application process, revocation process, or both. The RA does not need to be a separate body, but can be part of the CA.

Responsibilities that could be allocated to an RA include:

- Validate the identity of the entity requesting a public key certificate, according to the CA's Certification Practice Statement (CPS);

Subscriber

The Subscriber has some obligations, which should be covered in the agreement between the CA and the subscriber according to contractual agreements, including:

a) the subscriber should undertake to follow the certain procedures when applying for a certificate;

b) the subscriber should retain control of its private key, protect it in accordance with applicable parts of the certificate policy definition, and take reasonable precautions to prevent its loss, disclosure to any other party, modification, or unauthorised use;

c) the subscriber should report to the CA upon any suspicion that the key may have been compromised;

d) the cryptographic token, on which private keys are stored, should be protected to an extent comparable with that of valuable personal items such as credit cards or a driver's license. The PIN or password used to unlock the token must never be stored in the same location as the token itself; and

e) subscribers should not leave their cryptographic token unattended in an unlocked state (i.e., unattended in a workstation when the PIN or password has been entered).

Relying Parties

a) A disclosure Statement shall include a notice that if it is to reasonably rely upon a KeyOne TWS Certificate, the relying party shall be informed of the reasonable steps to be taken to verify the authenticity and validity of a certificate, using current certificate validation process, as indicated:

    a. From certificate information:

        - Check the correct signature of the certificate from a trusted certification authority

        - Check the current validity of the certificate, to ensure certificate status information is provided by the CA issuer



b. From revocation status information:

- Check Certificate Revocation status through VA services.

Notice that depending on KeyOne TWS's practices and the mechanism used to provide revocation status information, there may be a delay in disseminating the revocation status information. This delay will depend on the nature of the information being certified.

The maximum delay between receipt of a revocation and/or suspension request and the change to certificate status information shall not exceed 24 hours.

The propagation time from the Revocation Management Service to Revocation Status Service implies the updating of the keyOne VA component. The recommendation of the synchronization time between these two services is 2 hours.

b) Take any other precautions prescribed in agreements or elsewhere.

It is the responsibility of the Certificate Authority to ensure that any limitations governing the reliance on Certificates or limitations conditions on liability are clearly brought to the attention of any relying party

Time Stamping Service

The TSA should:

a) guarantee only the trusted source of time;

b) include a monotonically (never increasing or never decreasing) incrementing value of the time of day into its time stamp token (the time chosen to be used may be world time GMT or local time);

c) produce a time stamp token upon receiving a valid request from the requester;

d) include within each time stamp token an identifier to uniquely indicate the trust and validation policy under which the token was created;

e) time stamp only a hash representation of the message;

f) sign each time stamp token using a key generated exclusively for this purpose and have this property of the key indicated on the corresponding certificate (cryptographic methods other than signing can also be used);

g) provide a signed or otherwise verifiably secure receipt in the form of an appropriately defined time stamp token to the requester, where appropriate, as defined by policy.

Certificate Management Guidelines

Certificates issued under this policy may be used to support electronic signatures which "satisfy the requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper based data", as specified in article 5.1 of Directive 1999/93/EC [Eur99b].

Certificate Application

Registration procedures must be defined to fulfill [TS101456], verifying by appropriate means the identity of subscriber and any other specific attributes of the person to which a NQC or QC is issued.

All the subscriber information affected by data protection requirements must be protected from disclosure during registration process and when being forwarded to the Certificate Generation Service.

To this extent, Registration Officers must be aware of their duties managing subject sensitive information.

Certificate Generation

RAs and CAs are to take reasonable care in accepting and processing Certificate applications. They are to comply with the practices described in this CPS and with any requirements imposed by the CP under which the Certificate is being issued.

In particular, care should be taken to ensure Certificate information does not contain any factual misrepresentations and that no data entry errors are made when accepting an application or generating a Certificate.

RAs and CAs are not responsible for monitoring, investigating or confirming the accuracy of Certificate information after a Certificate has been issued. Where advice is received that Certificate information is inaccurate or no longer applicable, the Certificate may be revoked and a new Certificate applied for.

Certificate Suspension and Revocation

Circumstances for revocation

Revocation can be described as no longer being able to use a Certificate. A service provider or End Users' Certificate is revoked when:

1. The Certificate owner or their keys or Certificates are compromised through:
   - the theft, loss, disclosure, modification, or other compromise or suspected compromise of the user's private key(s);
   - the deliberate misuse of keys and Certificates, or a substantial non-observance of operational requirements in the subscriber agreement or associated CP or of the practices in this CPS;
2. A Certificate owner leaves the community of interest, for example:
   - an organizational End User leaves the employment of their organization;
   - a service provider ceases operations;
   - the decease of an End User;



3. There is an improper or faulty issue of a Certificate due to:
   - a material prerequisite to the issue of the Certificate not being satisfied;
   - a material fact in the Certificate is known or reasonably believed to be false;
   - data entry or other processing errors;
4. The Certificate of a superior RA or CA is revoked;
5. It is known or there is reason to believe a service provider does not possess the financial resources to maintain its Certificate services.

Circumstances for revocation or suspension

End Users may request the revocation of their own Certificates for any reason, and must make such requests through an authorised RA.

Authorised third parties may also request Certificate revocation through an authorised RA. Such authorised parties include, but are not limited to:

Note that a court order for Certificate revocation may be served directly on an issuing CA.

CRL distribution procedure

A manual and promptly distribution procedure of CRLs must be put in place to update those components which can not be automatically replace.

Certificate Renewal

The validity period of certificates will be determined depending of the type of certificates and the risk exposures of related secret keys.

Infrastructure[136] and control[137] keys will be renew on a regular basis.

When a secret key is compromised for any reason or a key changeover is required, a new certificate must be issued. This is applicable to signing, infrastructure[138] and control[139] keys.

---

[136] *Infrastructure keys are used by the some TOE components for processes such as subsystem authentication, audit log signing, encrypting transmitted, …*

[137] *Control keys are used by personnel managing or using the TOE components, and that may provide authentication, signing or confidentiality services for those personnel interacting with the system.*

[138] *Infrastructure keys are used by the some TOE components for processes such as subsystem authentication, audit log signing, encrypting transmitted, …*

[139] *Control keys are used by personnel managing or using the TOE components, and that may provide authentication, signing or confidentiality services for those personnel interacting with the system.*

Archival

To comply with all the archiving requirements auxiliary storage mechanisms are required. The processing, administration and management process of this archiving must ensure sufficient storage capability to maintain the records during the time retention period. The database administrator must periodically verify the available storage capability, and assign the necessary resources to the database, in order to the system successfully records all the required information.

Security Audit procedures

All approved CAs, RAs, TSAs and VAs are obliged under contract to maintain, adequate records and archives of information pertaining to the operation of the public key infrastructure.

TOE software preserves an audit trail for the events (the administrator configures this data in the start-up phase), but authorized access to this information must be enforced by procedural and administrative means, with the support of operating system and databases security mechanisms.

Systems and Operations Guidelines

In practice an assessment should be carried out to identify the level of risk associated with the TOE services to be implemented. The type and strength of security requirements to be selected will depend on the specific services provided by the TOE as well as on the risks involved in case the TOE services should become compromised. The security requirements associated with these identified risks should be specified in the TOE's security policy. This assessment and policy development should include the following

Physical Security

Main issues to be considered in the establishment of a System Security Policy aligned with the Security policy of the Service Provider are pointed out.

Equipment and Information Security

To prevent loss, damage or compromise of assets and interruption to business activities, equipment should be physically protected from security threats and environmental hazards

Power and air conditioning

The TOE secure operating area is connected to a standard power supply. All critical components are connected to uninterrupted power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure.

The area has an air conditioning system to control the heat and humidity that is independent of the building air conditioning system.



High availability services within the TOE employ appropriate power supplies and air conditioning systems to protect the uninterrupted provision of their services.

Clear desk and clear screen policy

In order to reduce the risks of unauthorized access, loss of, and damage to information during and outside normal working hours, the following policy guidelines must be applied:

1. Computers terminals and printers should not be left logged on when unattended and should be protected by key locks, passwords or other controls as shutdown when not in use.
2. Sensitive or classified information, when printed, should be cleared from printers immediately
3. Sensitive information should be locked away when not required, especially when the office is vacated.

Procedural Controls

1. ACCESS CONTROL MECHANISMS. Users, administrators and operating personnel of the TOE should only have access to information and resources they are entitled to. This is also applicable to database access which store audit records or other archiving systems and must be enforced by system operating level security mechanisms or by secure configuration of database systems.
2. IDENTIFICATION & AUTHENTICATION. The administrative procedures should ensure the unique and secure identification, and registration of users and operators of the TOE services;
3. CONFIDENTIALITY MECHANISM. Highly sensitive information, which is fundamental for the trust in the TOE, such as signing and infrastructure[140] keys, should be generated, installed and managed by well-documented and trustworthy procedures. To this extent, the use of Hardware Security Module to support CA, VA y TSA private signing keys, compliant with FIPS 140-2 level 3;
4. ACCOUNTING. In order to ensure the traceability of operations and transactions and the accountability of entities, the following measures should be taken with the required strength:
   - authentication of entities;
   - electronic signature of all security sensitive requests, transactions and operations; and
   - restrict auditing data to the proper authorities (e.g., security auditors). This access control must be enforced by the operating system and database management system as pointed out in the first paragraph.

[140] Infrastructure keys are used by the some TOE components for processes such as subsystem authentication, audit log signing, encrypting transmitted, …

– Clock synchronization, to ensure the accuracy of audit logs, which may be required as evidence in legal or disciplinary cases.

5 In order to protect the privacy and business interests of all the involved entities, information at interfaces, carried by protocols and on storage media, should have the required level of integrity and confidentiality protection;

6 System security, including operating system security, of all components governed by the security policy of the TOE should provide the necessary protection in the actual operating environment;

7 Adequate security management should cover the initiation, monitoring and control of the security services protecting the services provided by the TOE;

8 Procedures should be available to recover to a secure state in case of a security breach. This also implies the recovery or replacement of top-level secret key(s) of the TOE;

9 Mechanisms should be in place to safeguard against any single point of vulnerability that might exist in systems where a TOE is able to recover the encrypted data by using key recovery;

10 If required by the security policy of the entities involved, the TOE should provide the means to ensure that only keys needed by an authorised entity can be recovered by the TOE; and

11 Recovery procedures should also include minimising the impact to the entity through appropriate notification procedures.

12 Time Synchronization. Because of issuing and managing certificates are time related, all clocks of the TWS components must be synchronized to within 1 second of an UTC independent source.

Personnel Security

Training requirements

Effective information security awareness, training and education should be required by all TOE users and administrators to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of certification processes.

All TOE internal users (operators and administrators) are trained in the:

- Use and Administration of KeyOne CA Application
- Use and Administration of KeyOne LRA Application
- Use and Administration of KeyOne TSA Application
- Use and Administration of KeyOne VA Application

SECURITY AWARENESS PROGRAM



Without the acceptance and involvement of personnel at all levels, a security awareness programme cannot succeed. It is especially critical for management to be aware of the need for security and to promote the awareness of security for their staff. The aim of an awareness programme is to convince personnel of the potential security risks and exposures in the TOE operations and systems. In particular personnel in frontline service , shall be informed of ty pical social engineering attacks and the safeguards against them.

Business Continuity Management

In order to counteract interruptions to certificate management activities (mainly dissemination service, revocation management service and revocation status service), ensure a promptly revocation and validation processes and protect critical processes from the effect of major failures or disasters, specially in cryptographic key management processes, a business continuity plan must be established.

Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

Following consideration must be done:

- Routine procedures will be established for carrying out the agreed back-up strategy, taking back-up copies of data and rehearsing their timely restoration, logging events and faults.
- Emergency procedures, manual fallback plans and resumption plans should guarantee a high level of availability in specific services as dissemination service, revocation management service and revocation status service.
- With regards to signing or private keys of the Certificate Generation Service, they would be stored and backed up only following an authorization mechanism based on N of M, where N components parts out of a total of M components parts are required for successful operation.
- Alternative TWS's must be used in case of disaster to continue operations providing an acceptable delay in service resumption.
- Formal contract arrangements with vendors to provide services in event of need to recover, including back-up site facility or relationship, in advance of actual need
- Cryptographic Keys Recovery Procedures must follow the guidelines and recommendations specified by HSM manufacturer to ensure recovery options and adequate security level.
- The responsibilities of the individuals, describing who is responsible for executing which component of the plan.

Technical Security Controls

Life cycle management of HSMs

The KEYONE TWS shall ensure the security of cryptographic hardware throughout its lifecycle.

In particular the KEYONE TWS shall ensure that:

a) the cryptographic hardware is not tampered with during shipment;

b) the cryptographic hardware is not tampered with while stored;

c) the installation and activation of the KEYONE TWS's certificate signing cryptographic hardware shall require simultaneous control of at least two trusted employees;

d) the configuration of HSM must have recovering properties activated.

f) the generation, activation, back-up and recovery of the KEYONE TWS's signing keys in cryptographic hardware shall require simultaneous control of at least two trusted employees, including a Security Officer role;

g) the cryptographic hardware is functioning correctly; and

h) KEYONE TWS private signing keys stored on KEYONE TWS cryptographic hardware are destroyed upon device retirement Key Pair Generation and Installation

Key pair generation

Service Provider key pairs are generated and installed by the KeyOne LRA

End User key pairs will be generated by an authorized Registration Officer, using Card Management Systems to generate smartcards with all signature creation data on it and ready to be activated by its owner. These keys will be generated and installed by KeyOne LRA component.

Registration Officer signing keys will be generated following the same procedure described for end users, except for the distribution mechanism of the keys to be certified by certification authority which must be offline and usually performed by an authorized personnel as the CA administrator[141].

CA, VA, TSA keys are generated and stored in HSM's. This HSM must be certified FIPS 140-2 level 3. If a Secure Cryptographic Device is used in these entities, then this device must be certified ITSEC E4.

LRA keys are generated and stored in a Secure Cryptographic Device that is certified ITSEC E4.

[141] *only applied in the first registration officer of the infrastructure.*



The VAs (certificates of OCSP signing) must be certified by a Certification Authority trusted domain.

Private key delivery to entity

Self-generated private keys do not require delivery.

The End user signature-creation data are generated and stored by an RA using a Secure Cryptographic Device certified ITSEC E4, which will be distributed in a secure manner to ensuring that secret keys are always protected from disclosure. These SCD must be conformant with [CEN01b] fulfilled the requirements identified in Annex III of [Eur99b]. SCD activation data is considered sensitive information which must also been generated and distributed in a secure manner to ensure the SCDev can not be misused by CSP's personnel.

Public key delivery to certificate issuer

Public keys generated during process registration are distributed to KeyOne CA for certification via protected certificate requests communication link.

CA public key delivery

The CSP public keys required by an End User may be distributed with the End User's own keys and certificates or may be downloaded by the End User from the Directory.

When delivering and installing root certificates into others Private Secure Store components, manual verification of the authenticity and integrity is required. An appropriate control mechanism is to check the hash certificate or its fingerprint from a reliable source.

When the fingerprint mechanism was used in order to check the integrity of the certificates installed in the applications, then only an strong algorithm will be used in this verification; consequently the SHA1 algorithm will be used for this purposes.

Private Key Protection

FIPS 140-2 level 3 Validated hardware modules provides a secure management and storage of private keys through a tamper resistant device.

The administration of keys are controlled by strong authentication mechanisms as smartcards providing a highly flexible means of sharing responsibilities between individuals within the organization.

To avoid intentionally misuse of key management processes, two-factor authentication, split responsibility and role separation are implmented by threshold sets of smartcards. These means "n" of a total of "m" smartcards[142] must be presented to authorize an specific cryptographic function or administrative activity.

[142] *Where n is greater or equal than m, and n>1.*

A failover capability is required for this HSM's, to pass all the processing activities to another module in case of unavailability of fatal error.

Web Clients Encryption Requirement

High-encryption modules must be installed in web clients to establish secure sessions with server applications[143].

Activation Data

Activation data generation and installation

No activation data other than access control mechanisms is required to operate cryptographic modules.

An End User Personal Identification Number (PIN) may be generated by an RA during key pair creation, to protect the transport of an End User's keys and certificates to the End User.

Activation data protection

No activation data other than access control mechanisms is required to operate cryptographic modules.

PINs must be supplied to End Users in a secure manner, for example by a blind-envelope, to provide increased security against third party interception of the PIN.

Computer Security Controls

Specific computer security technical requirements

Service Provider has established an approved System Security Plan that incorporates computer security technical requirements that are specific to that Service Provider's operations.

Computer security rating

Service Provider has established an approved System Security Plan that incorporates computer security ratings that are specific to the CA.

---

[143] *Only 3DES and RC4-128 symmetric algorithms are accepted.*



Life Cycle Technical Controls

System development controls

Service Provider and End User Client applications are developed in controlled environments employing appropriate quality controls.

Security management controls

System security management is controlled by the privileges assigned to operating system accounts, and access control of databases management systems

Life cycle security ratings

Service Provider must establish an approved Protective Security Risk Review that identifies and addresses all high or significant life cycle security threats.

In deploying or migrating TWS components, controls must be put in place to minimize system failures. They should ensure that all proposed system changes are reviewed to check they do not compromise the security of either the system or the operating environment. The following are examples of that:

- Change Control Procedures, to minimize corruption of information systems, controlling implementation changes
- Technical review of operating system changes, to ensure there isn't, no adverse impact on operation or security of applications.
- Detection and prevention controls to protect against malicious software and appropriate user awareness procedures.

Network Security Controls

Service Provider has established an approved Protective Security Risk Review that identifies and addresses all high or significant network security threats.

I3D Database Security Controls

The only authorized person to administer TOE databases are the specific operators of TOE application (CA, TSA y VA). No one I3D[144] master entity must be created in start-up process.

[144] *The I3D Database is a KeyOne technological mechanism for protecting the integrity of the KeyOne databases.*



SAFELAYER SECURE COMMUNICATIONS, S.A.

Edificio Valrealty C/ Basauri, 17 Edifico B Pl. Baja Izq. Of. B 28023 Madrid (SPAIN) Tel.: +34 91 7080480 Fax: +34 91 3076652
Edif. World Trade Center (S-4), Moll de Barcelona S/N 08039 Barcelona (SPAIN) Tel.: +34 93 5088090 Fax: +34 93 5088091

WWW.SAFELAYER.COM